

SECURITY

INTRODUCTION

This is a manual for those who intend to destroy the state and capital (and patriarchy and white supremacy and...), but it is also for those who understand that the state and others opposing us will fight back.

We know that the first weapons used against us are in the classroom or via TV commercials and newspaper commentaries. Calling someone an “eco-terrorist”(a term invented by the FBI and popularized by the Oregonian) is an ideological attack. Calling the new youth culture that confronted fascists in the Northwest “gang members”(again, the Oregonian) was also wielding a weapon.

We are not dealing mainly with these types responses here. They are primary in modern capitalist society, but it is a mistake to believe that they constitute the spectrum. This manual looks at other tools at hand: surveillance, police informers, provocateurs and infiltration of organizations as well as the strategies behind the state's repression.

Our criticisms of parliamentary strategies for overthrowing capital exist in other forums, but it should be remembered that the illusion of being protected extends deeply among trade unionists, student activists and community organizers. Real confrontation or real movement reveals that the tactics of surveillance, cooptation and repression are still being used, though certainly not with the openness that they are brought against members of the black bloc, forest defenders, abolitionists, Muslims, and those who defy ICE.

A new generation of activists has come into existence that organizes via laptops and cellphones, Twitter, Facebook and texting. According, simple measures such as “Pick a good password” are promoted as security strategies.

We think good passwords are a good idea. The extension of this good tactic into an entire strategy is a problem, however. In-depth seminars on how to protect all electronic data are regularly held at all types of 'movement' gatherings, sometimes ignoring the openly known fact that ALL electronic communication in the world can be intercepted, stopped, or mimic'ed and altered. The simple method of stealing a laptop or seizing it in an FBI raid makes a mockery of all the precautions that don't acknowledge this possibility. Organizations and movements that have not understood this have already been decimated as their tools are turned into weapons against them.

Finally, if this manual succeeds only in destroying the prevalent “common sense” of 'security culture', it will have been worth all its work.

It is noteworthy that those locations and political spaces that have most promoted 'security culture' have suffered the worst political defeats by the FBI. We refer to Eugene, Oregon and Earth First as well as the ELF.

The strategy inherent in 'security culture' as promoted in militant circles leads to a separation of a movement from a populace, then separation of an organization from a movement, then a cell from the organization, then, inevitably, individuals from the cell. Few of those who have promoted this realize that the strategy of the 'lone wolf' is fascist in origin. We think its recent track record in keeping activists safe and free stands for itself in regards to its failures (this cannot be taken as an aside from the serious political flaws inherent within the approach).

It is our belief that effective security may involve organizational apparatus, practices, and cultures, but at its heart, requires that all members of political organization be equipped with the theoretical grounding, critical thinking apparatus, and collective processes necessary for evaluating threats and responses, both on a local and individual level, and on a movement level.

Despite the devastation of the Green Scare, the proponents of 'security culture' argue that it should be practiced more rigorously. Thus recent and future anarchist gatherings will occur where attendees are not being told of the location until arrival at a secure checkpoint". This method , also in use by neo-fascist groups in the U.S., is easily breached. But it eliminates any notions of mass organizing. It is as though "Anna", a teen-aged kid armed only with a tattoo and some,"grubby clothes," had not already infiltrated every significant anarchist gathering across the U.S., reported back to the FBI, and led a string of actions and campaigns that led to the incarceration and terrorization of a large community of well-intended young people.

We can do better. If we take seriously the urgency of this moment and the tasks before us, we absolutely must.

The most important thing to emphasize in developing a sense of good movement and organizational security is that a democratization of knowledge and critical thinking skills is essential.

USING THIS PACKET

This guide will only be effective if those reading it actually prepare before group study-this means answering each question for the relevant section, to the best of one's ability, and coming prepared to discuss and debate each others responses. This practice is the core of what makes good security-the ability to collectively and independently analyze a situation, threats, and the compromises which a response entail under varying conditions. We pose this in stark contrast to the prevailing wisdom in our circles, where a rigid series of cloak and dagger behaviors and technologies are posed as,"security culture." Schneier's writings, both in this compilation, and elsewhere, do well at emphasizing this.

Folks should do the readings, viewings, and listen to the audio recommendations before each discussion, and should write out responses to the questions in each section before they come to the study group. There are no right/wrong answers. The key here is to force each student to grapple with the frameworks we hope the materials provide. These frameworks are essential to guiding the critical thinking process which is the heart of good security. Study group participants can then take turns answering questions, with the rest of the group responding, challenging, or building off the first answer.

The goal of coming together as a study group for each section will be to challenge each others responses and interpretations to each question, and to fill in areas where individuals may have gaps in understanding. It is also important to begin the actual practice of debating and evaluating threats and responses in a collective format-that even if organizational demands require that specific organizational members be devoted to prioritizing these tasks, that the entire membership of political organization must constantly be involved in the process of evaluating and responding to real or potential threats.

There are two types of questions included in the study response-those with relatively simple interpretations and answers, and those oriented around a collective brainstorm of solutions and responses to what are both political and technical questions. We don't expect this to be easy.

The practice of debating and grappling with these questions, first individually, then as a collective, are central to shattering the rigid conceptions of,"security culture," which have left organizations and groupings so vulnerable to manipulation and disruption. The most important thing we want to emphasize is that good security is not a matter of: Choose A, B, C, or D. Its not encryption, its not good passwords or codes, and its certainly not going to be found in technologies or rigid rules. Although all or any of these may be useful components of a security system as a whole, if they become the system itself, these very technologies and approaches will often become the crucial vulnerabilities which defeat that very system.

Table of Contents

Part One: Principles of Security	1-7
Study questions.....	1
Bruce Schneier, <i>Beyond Fear</i> (Copernicus Books, 2003), pages 11-16.....	2-7
Part Two: Understanding Repression	8-76
Study Questions.....	8
Ken Lawrence, <i>The New State Repression</i> (Tarantula, 2006).....	9-24
Kristian Williams, <i>Other Side of the Coin</i> (unpublished).....	25-76
Part Three: Social Engineering and Pseudo Ops	77-141
Study Questions.....	77
Kevin Mitnick, "Social Engineers," <i>The Art of Intrusion</i> (Wiley Publications, 2005). .	78-102
Lawrence E. Cline, "Pseudo Operations And Counterinsurgency: Lessons From Other Countries," (Strategic Studies Institute, June 2005). .	103-139
Part Four: Approaches to Security	78-185
Study Questions.....	140-1
Anti-Repression Resource Team and Midwest Research Group, <i>Protecting Ourselves from State Repression, Volume One: Organizational Security</i> (1983). .	142-159
Elaine Scarry, "Citizenship in Emergency," from <i>The Best American Essays 2003</i> , ed. Anne Fadiman (Houghton Mifflin, 2003). http://www.bostonreview.net/BR27.5/scarry.html .	160-177
Naomi Klein, <i>The Shock Doctrine</i> (Metropolitan Books, 2007).....	178-80

Anonymous, *Got the Hollow Points for the Snitches* (self-published, undated)..181-5 **Part Five: Informers,**

Infiltrators, and Provocateurs186-205

Study Questions.....186-7

Thomas Cincotta, "From Movements to Mosques, Informants Endanger Democracy," *The Public Eye* (Summer 2009).

<http://www.publiceye.org/magazine/v24n2/movements-to-mosques.html> ...188-193 Michael William, "Portrait of a Police

Infiltration," *Anarchy: A Journal of Desire Armed* (Fall/Winter 2001-2002). 194-5 Denny Walsh, "Leader or Led by the FBI?" *Sacramento Bee*, September 26, 2007...196-7

Michael May, "Turncoat: My Way or the FBI Way," *This American Life*, May 22, 2009,

<http://www.thisamericanlife.org/radio-archives/episode/381/Turncoat> ...available only on internet

Andrea Todd. "The Believers," *Elle*, " April 2008.....198-205

Courtney Desiree Morris, "Why Misogynists Make Great Informants," *Make/Shift* (Spring/Summer 2010).

<http://inciteblog.wordpress.com/2010/07/15/why-misogynists-make-great-informants-howgender-violence-on-the-left-enables-state-violence-in-radical-movements/>206-212

Part Six: Review and Role Plays213-4

Part Seven: Postscript-

Victor Sergei,"Conclusion: Why The Russian Revolution Was Still Invincible," *What Every Radical Should Know About State Repression*, (Ocean Press, 2005).....215-222

Study Questions

Schneier

1- Schneier's definition of security suggests that "we want people to behave in a certain way" and security is the means that we use to make sure they do.

In what ways does your organization want to make sure that people behave? How do your existing security measure ensure that they do? Is security necessarily repressive, or can it be consistent with liberatory politics?

2- In interviews after September 11, Schneier was asked how the government could guarantee that there would never be a similar attack. His snarky response: "Ground all planes forever." What is Schneier trying to demonstrate here? Why wouldn't that be a feasible approach? Is there something wrong with the original question? Given that security is always a trade-off, is absolute security possible? Is it even desirable?

3- Schneier distinguishes between security and safety based on the intentions of the agents involved. Does this distinction hold up in practice? How does it function when you don't know the intentions of the people involved?

4- Answer Schneier's five questions as they relate to your organization. Keep this list for future reference: What assets are you trying to protect? What are the risks to these assets? How well does the security solution mitigate those risks? What other risks does the security solution cause? What costs and trade-offs does the security solution impose?

Security is complicated and challenging. Easy answers won't help, because the easy answers are invariably the wrong ones. What you need is a new way to think.

....

All security is, in some way, about prevention. But prevention of what, exactly? Security is about *preventing adverse consequences from the intentional and unwarranted actions of others*. What this definition basically means is that we want people to behave in a certain way—to pay for items at a store before walking out with them, to honor contracts they sign, to not shoot or bomb each other—and security is a way of ensur-

ing that they do so. Obviously, if people always did what they were supposed to do, there would be no need for security. But because not everyone does, security is critical to every aspect of society. The definition above tries to bring these issues into focus.

- Security is about prevention. A *security system* is the set of things put in place, or done, to prevent adverse consequences. Cars have anti-theft security systems. The money in your wallet has a variety of anti-counterfeiting security systems. Airports and airplanes have many overlapping security systems. Some security systems, like financial audits, don't stop criminals but reduce or prevent the adverse consequences of their crimes. (This type of after-the-fact security system has a deterrence effect, which acts as a form of prevention.) Like any other system, security systems can be attacked, can have flaws, and can fail.
- Security concerns itself with *intentional* actions. This points to an important distinction: Protecting assets from unintentional actions is safety, not security. While it is common to talk about securing ourselves against accidents or from natural disasters, in this book I try to restrict the discussion to security from intentional actions. In some ways this is an arbitrary distinction, because safety and security are similar, and the things that protect from one also protect from the other. And, in fact, safety is often more important than security, since there are far more unintentional unwarranted actions in the world than intentional ones. I make the distinction for the purpose of limiting the scope of this book.
- These intentional actions are *unwarranted* from the point of view of the *defender*. Note that the unwarranted actions are not necessarily illegal.
- Security requires the concept of an *attacker* who performs these intentional and unwarranted actions. It's important to understand that this term is meant to be nonpejorative, value-neutral. Attackers may be on your side. Burglars are criminals, but police officers who attack a drug lord in his mountain hideout are the good guys. Sometimes the attacker isn't even human, as in the case of a tiger trying to pry open your Land Rover and eat you. The term *attacker* assumes nothing about the morality or the legality of the attack. It doesn't even imply malicious intent, although that certainly is often involved.

- Those intentional unwarranted actions are called *attacks*. An attack is a specific way to attempt to break the security of a system or a component of a system. It can refer to an abstraction—“You can successfully attack a house by breaking a window”—or it can refer to a specific incident—“On 7 September 1876, the Jesse James Gang attacked the First National Bank of Northfield in Northfield, Minnesota.”
- The objects of attack are *assets*. Assets can be as small as a single diamond and as large as a nation’s infrastructure.
- Security can also refer to the mechanisms used to provide the protection. In this book, the individual, discrete, and independent security components are called *countermeasures*. Countermeasures include door locks, guards, ID cards, and the metallic thread in banknotes that makes them more difficult to counterfeit. Walls, alarms, cryptography, pots of boiling oil you can pour on the heads of people invading your castle—these are all countermeasures. A security system consists of a series of countermeasures.

Unfortunately, many countermeasures are ineffective. Either they do not prevent adverse consequences from the intentional and unwarranted actions of people, or the trade-offs simply aren’t worth it. Those who design and implement bad security don’t seem to understand how security works or how to make security trade-offs. They spend too much money on the wrong kinds of security. They make the same mistakes over and over. And they’re constantly surprised when things don’t work out as they’d intended.

One problem is caused by an unwillingness on the part of the engineers, law enforcement agencies, and civic leaders involved in security to face the realities of security. They’re unwilling to tell the public to accept that there are no easy answers and no free rides. They have to be seen as doing something, and often they are seduced by the promise of technology. They believe that because technology can solve a multitude of problems and improve our lives in countless ways, it can solve security problems in a similar manner. But it’s not the same thing. Technology is generally an enabler, allowing people to do things. Security is the opposite: It tries to prevent something from happening, or prevent people from doing something, in the face of someone actively trying to defeat it. That’s why technology doesn’t work in security the way it does elsewhere, and why an overreliance on technology often leads to bad security, or even to the opposite of security.

The sad truth is that bad security can be worse than no security; that is, by trying and failing to make ourselves more secure, we make ourselves less secure. We spend time, money, and energy creating systems that can themselves be attacked easily and, in some cases, that don't even address the real threats. We make poor trade-offs, giving up much in exchange for very little security. We surround ourselves with security countermeasures that give us a feeling of security rather than the reality of security. We deceive ourselves by believing in security that doesn't work.

....

Security is complex, but complex things can be broken down into smaller and simpler steps. Throughout this book, I use a five-step process to analyze and evaluate security systems, technologies, and practices. Each of these five steps contains a question that is intended to help you focus on a particular security system or security countermeasure. The questions may seem, at first, to be obvious, even trivial. But if you bear with me, and take them seriously, you will find they will help you determine which kinds of security make sense and which don't.

- *Step 1: What assets are you trying to protect?* This question might seem basic, but a surprising number of people never ask it. The question involves understanding the scope of the problem. For example, securing an airplane, an airport, commercial aviation, the transportation system, and a nation against terrorism are all different security problems, and require different solutions.
- *Step 2: What are the risks to these assets?* Here we consider the need for security. Answering it involves understanding what is being defended, what the consequences are if it is successfully attacked, who wants to attack it, how they might attack it, and why.
- *Step 3: How well does the security solution mitigate those risks?* Another seemingly obvious question, but one that is frequently ignored. If the security solution doesn't solve the problem, it's no good. This is not as simple as looking at the security solution and seeing how well it works. It involves looking at how the security solution interacts with everything around it, evaluating both its operation and its failures.
- *Step 4: What other risks does the security solution cause?* This question addresses what might be called the problem of unintended consequences. Security solutions have ripple effects, and most cause

new security problems. The trick is to understand the new problems and make sure they are smaller than the old ones.

- *Step 5: What costs and trade-offs does the security solution impose?* Every security system has costs and requires trade-offs. Most security costs money, sometimes substantial amounts; but other trade-offs may be more important, ranging from matters of convenience and comfort to issues involving basic freedoms like privacy. Understanding these trade-offs is essential.

These five steps don't lead to an answer, but rather provide the mechanism to evaluate a proposed answer. They lead to another question: Is the security solution worth it? In other words, is the benefit of mitigating the risks (Step 3) worth the additional risks (Step 4) plus the other trade-offs (Step 5)? It is not enough for a security measure to be effective. We don't have limitless resources or infinite patience. As individuals and a society, we need to do the things that make the most sense, that are the most effective use of our security dollar. But, as you'll see later in this book, subjective (and sometimes arbitrary) economic incentives make an enormous difference as to which security solutions are cost-effective and which ones aren't.

These five steps may seem obvious when stated in this abstract form, but applying them to real situations is hard work. Step 3, for example, requires you to understand the security solution and how well it actually works—not merely as described in the manufacturer's literature or as explained to you by a politician, but in real situations against real attackers. Step 5 requires you to understand the variety of trade-offs a security solution imposes, how it interacts with other aspects of your life, and what ancillary security solutions are required to make it work. The answers aren't always easy to come by. It's hard to quantify any of the steps, including the threat. Sometimes you won't have enough information, and you will be forced to make your best guess. Sometimes you'll be comparing apples and oranges. It can quickly become very complex and subjective.

Keep the steps in mind as you read the many examples in this book, and as you encounter and interact with the thousands of security systems that surround you every day, you'll start to notice the difference between good and bad security or security that could be designed better or require less onerous trade-offs. You'll begin to realize how ineffectual some common security systems are: how they solve the wrong problem or cause more problems than they solve. You'll start

making different security decisions: choosing more security in some instances and less security in others. You'll become more aware of the security trade-offs being imposed on you. And because security is all of a piece, the same knowledge will make you better able to choose a home alarm, and better equipped to participate in the national security policy debates.

Lawrence

- 1- Outline Kitson's three stages of insurgency. At which stage is the social movement of which you are a part? How is Kitson's conception of insurgency different from older views? What does this imply about society? What are the implications for social movements?
- 2- What does the map of San Luisa (page 14) show us about the state's aims and strategy? How does its strategy reflect Giuffrida's social theory?
- 3- Distinguish Eveleigh's approach from Kitson's. Which to you see employed in the US?
- 4- Re-read Eveleigh's instructions for recruiting informers (pages 20-1). How could resistance groups guard against this?

Williams

- 1- Review the stages of Insurgency (pages 6-8). Which stage is the current social movement in? Which stage do the state's actions seem aimed at addressing?
- 2- Williams characterizes the state's main intelligence needs as sociological rather than conspiratorial. What does this suggest about your organization's intelligence needs? What does it suggest about the need for, or uses of, secrecy? What needs to be secret, and from whom?
Refer specifically to Table 3-9 (page 10).
- 3- Historically, a major weakness of the state has been in understanding how movements are organized. Much present counterinsurgency work involves social network analysis and social mapping. What has the emergence of social media sites like Facebook changed in this regard? What new possibilities do these sites open for the repressive agencies? How does your organization weigh the benefits and risks of using these technologies?
- 4- Consider Williams' conclusions. What lessons does he offer for social movements? Do you agree? How does his perspective relate to the work of your organization?

Today's political repression differs fundamentally from the repression practiced around the world in the past. The most basic difference is on the level of *strategy*—the general approach of the state, the outlook of the ruling class.

Their belief is that insurgency is not an occasional, erratic idiosyncrasy but a constant occurrence—*permanent insurgency*, which calls for a strategy of *permanent repression* as the full-time task of the security forces.



2006 edition by:

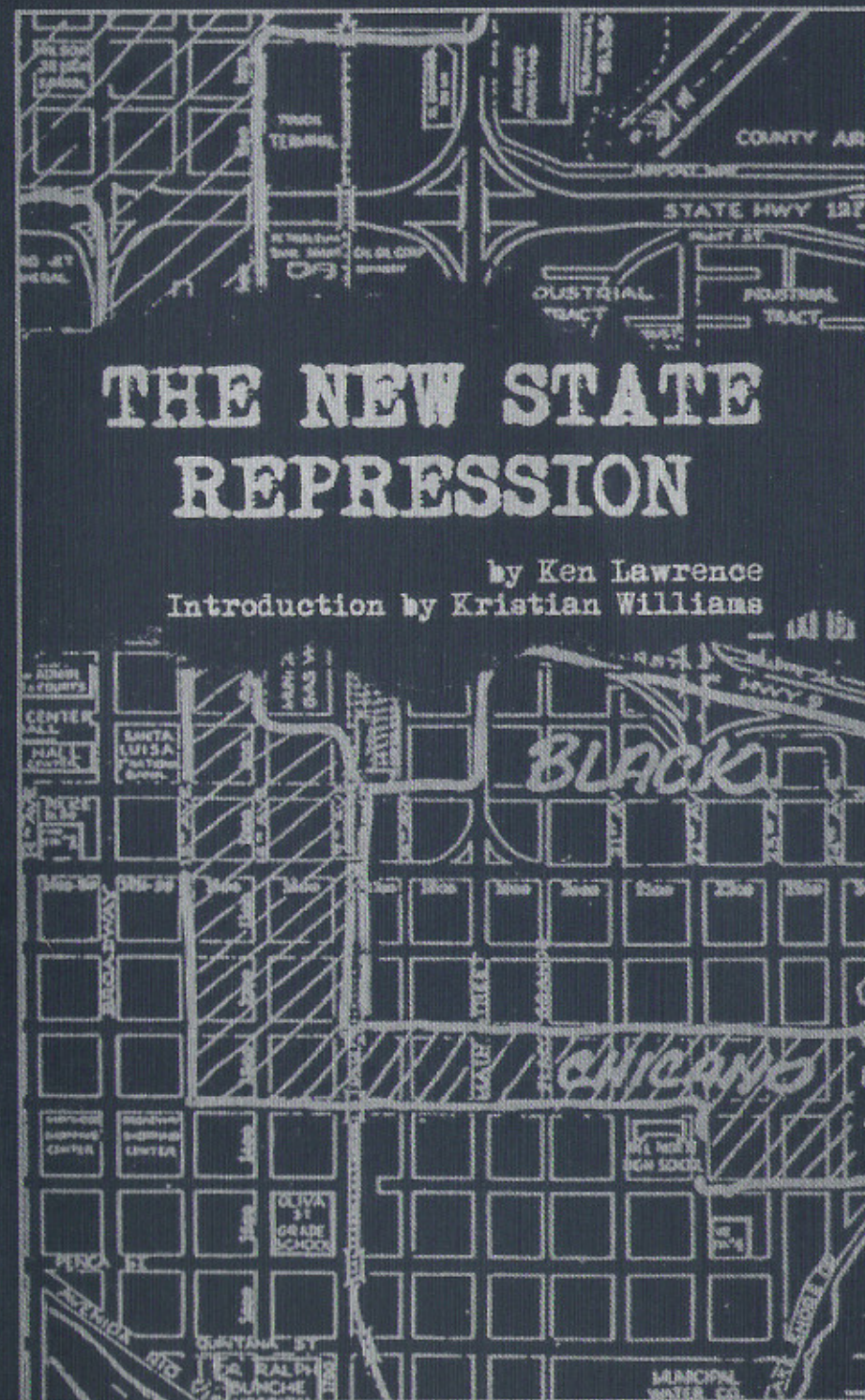
Tarantula

Publishing & Distribution

818 SW 3rd Ave. PMB #1237

Portland, OR 97204

www.socialwar.net



References

Repression Strategies:

California Specialized Training Institute, "Civilian Violence and Terrorism: Officer Survival and Internal Security." (Lecture/syllabus). CSTI: Camp San Luis Obispo, California, revised August 1974.

Eveleigh, Robin, *Peace-Keeping in a Democratic Society: The Lessons of Northern Ireland*. C. Hurst & Company: London, 1978.

Federal Bureau of Investigation, *Proceedings of FBI International Symposium on Terrorism July 6-8, 1978*. FBI: Washington, 1978.

Kitson, Frank, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*. Faber and Faber: London, 1971

Kitson, Frank, *Bunch of Five*. Faber and Faber: London, 1977.

Anti-Repression Information and Analysis:

Ackroyd, Carol, Karen Margolis, Jonathan Rosenhead, and Tim Shallice, *The Technology of Political Control*. Pluto Press: London, revised edition 1980.

Lee, Edward A., "The Lumpenproletariat and Repression: A Case Study." In *Political Discussion*, Number 3. Freedom Information Service: Tougaloo, Mississippi, November 1976.

Ross, Caroline and Ken Lawrence, *J. Edgar Hoover's Detention Plan: The Politics of Repression in the United States 1939-1976*. American Friends Service Committee: Jackson, Mississippi, 1978.

Serge, Victor, *What Everyone Should Know About State Repression*. New Park Publications: London, 1979.

United Methodist Voluntary Service, *Repression and Resistance: The System vs. The People, An Information Manual*. (A packet of materials), UMVS: New York, 1982.

The New State Repression

Ken Lawrence

2006 Introduction by Kristian Williams

Tarantula
Portland, Oregon

"The New State Repression" was originally published by The International Network Against State Repression, 1985.

A slightly different version of this essay was printed in *CovertAction Information Bulletin*, Number 24 (Summer 1985).

Kristian Williams' introduction appears here for the first time.

A Few Words from the 2006 Publisher:

It is a pleasure to reprint Ken Lawrence's "The New State Repression," as well as to publish Kristian Williams' introduction for the first time.

The publisher does not agree with every sentence of this pamphlet. Such a total endorsement seems unnecessary, however, seeing as neither Lawrence nor Williams pretend to have the final word on state repression. As a general overview, "The New State Repression" has stood the test of time, and it ought to be carefully studied. The essay's subject matter deserves discussion both within, and also outside of, the political Left.

About copyright: until a truly human world community replaces market relations, the authors of this pamphlet reserve all their rights. If you wish to do a reprint for nonprofit purposes, please contact us beforehand.

Tarantula

818 SW 3rd Ave PMB #1237, Portland, OR 97204

www.socialwar.net

V. Conclusion

It is important for those of us who understand that we must fight repression not to skip any beats addressing the new realities, but we must adopt new strategies of our own to defend ourselves. It is not going to be an easy task. If we limit ourselves simply to having meetings and rallies and leafleting, we are going to see the Santa Luisa Five and the Other City Ten endlessly, until we're all safely packed away in concentration camps. We must help groups understand the new repression and train themselves to combat these incursions of the state while we continue to fight the political battles we all consider to be so important.

To begin, we must discard some of the left's conventional wisdom, particularly the assumption that the state's relatively tolerant attitude toward protest is permanent and the companion assumption that the defense of constitutional legality is sufficient to protect the political space required for the next mass insurgency to develop. Our assumptions about the potential of our movement must become at least as radical as those of the state, that there does exist an objective basis for insurgency, and that it can and must emerge.

The tasks that face us are complicated and difficult. We must recognize that we cannot hope to free today's grand jury resisters, political prisoners, and prisoners of war unless we can go the offensive against the new forms of repression; at best we will tread water, possibly freeing an occasional comrade as even more are carried off.

In an age when the police can hunt down revolutionaries by tracing their children's medical prescriptions, our opposition must be even more innovative. We do not claim to have all the answers, but we do believe we have identified the essential problem.

We urge activists to be in touch with us; we are eager to share what we have learned in the most constructive way we can.

We also need to understand that we cannot rely upon the traditional civil liberties organizations to help in this regard, because their strategies are too defensive, too little, too late. We've got to become the builders of a new movement, not simply a proliferation of *ad hoc* defense organizations each time we've got more prisoners of war or political prisoners to defend, but at the least the beginnings of an organized response that views thwarting the political police as a permanent task of our political work, in the same way that the bourgeoisie now views permanent repression as essential to its continuing rule.

Information request for the document, the FBI replied that no such thing exists. Fortunately it had already been captured and was in the hands of the dreaded "terrorists" by the time Andres asked for it.

The contents would surprise no one, so I won't quote a line of it here; the significance is in the attendance. Not only did this symposium convene high-level security officers from West Germany, the Netherlands, Italy, Japan, Spain, Portugal, Israel, and Great Britain, but it reached down into every village and hamlet throughout the United States. Nearly every FBI field office, state police department, and the chiefs or assistant chiefs of police from the hundred largest cities and towns in the U.S. were represented; a similar symposium was held in Puerto Rico.

This is new. Never before have the political duties of police on every level been so explicitly articulated, so broadly connected, so well organized. It is not just high technology that has made this possible; it is also the new strategies of permanent repression as articulated by Kitson and Evelegh.

Table of Contents

Introduction: Speaking of Repression by Kristian Williams	1
The New State Repression	
Author's Introduction	3
I. The Strategy of Permanent Repression	5
II. Frank Kitson in Theory and Practice	9
III. Louis Giuffrida: Ronald Reagan's Kitson	13
IV. Robin Evelegh's Alternative Strategy	17
V. Conclusion	23
References	24

because they are genuinely converted from their terrorist beliefs to supporting the Government cause.

Then he tells precisely how to use each of these five methods—torture, bribery, blackmail, induced cowardice, and conversion. He says they all work. Evelegh's appeal was obviously heard in Westminster, judging by the trials conducted in Belfast and Derry for the past few years based upon the evidence provided solely by paid perjurers induced to testify in these very ways, the so-called "supergrasses."

But that strategy has begun to unravel in the Irish context; even British judges have refused to accept some of the most important "supergrass" trial evidence as credible, and have released the defendants. In Italy, however, the induced testimony of the so-called *penitenti* has had a devastating effect on the armed revolutionary movement in that country. It is still too early to know whether its application in the United States will prove to be significant.

One important weakness in this aspect of Evelegh's strategy is that once activists are induced or coerced to betray their cause, they must be given permanent lifetime protection by the state—not an easy task at best, and especially complicated when the informer has become a recognized personality in the media. A chronic problem for the U.S. Witness Security Program is that, because so many of the informers are criminals, the effect of the program is to put the Justice Department in the position of indemnifying felons, even murderers, in exchange for testimony against others whose alleged "crimes" are minor by comparison, even to a public which supports the government and believes the witness.

Evelegh's strategy of repression, like Kitson's earlier, is being internationalized. A 1978 FBI document titled *Proceedings of FBI International Symposium on Terrorism* is especially interesting in this regard. Page two says,

Those who made presentations at the FBI International Symposium on Terrorism request that you do not duplicate this document in any way. Moreover, they request that information contained in their presentations not be disseminated outside your agency.

This admonition was taken so seriously that the FBI violated federal laws and its own regulations in a futile attempt to keep it secret. When Monica Andres of the Center for National Security Studies filed a Freedom of

It is difficult for those who have not been concerned personally with countering terrorism to understand the complete difference in quality and value between general information from the public and inside information from within the terrorist movement. ... Once their intentions are known to the Security Forces, the terrorists have lost the initiative; the Security Forces can then arrange reception committees for the perpetrators of acts of terrorism. It is only through inside informers that a terrorist organization can be exposed to this extent, and once so exposed it is helpless until it has discovered and removed the informers.

He then gives a detailed prescription for recruiting informers.

What is needed is the ability within the law to induce a terrorist to defect to the Government's side without his former colleagues knowing that he has done so, in return for indemnity for his crimes. We should consider briefly the effect on a terrorist organization of widespread publicity being given to official encouragement of defection in return for an indemnity. Any arrested terrorist will have his "easy way out" at the back of his mind if the pressures on him seem too strong. Whenever a terrorist is arrested, his colleagues will fear that he will defect and must take steps to protect themselves from the consequences of this with all the disruption that such hurried and unforeseen changes must cause...

Inside informers seldom appear of their own volition. They have to be consciously created, usually from among members of the terrorist organization who have been arrested...

Persuading a terrorist to defect is akin to the wooing of a woman—with persuasive and even glib arguments on one side, and on the other initial resistance and vacillation between the urge to consent and the urge to refuse, and if all goes well, the development of confidence. Indeed, the interrogator is seeking to achieve a seduction rather than a rape or a rebuff. ...

There seem to be five reasons why suspects are induced to think that it is in their best interests to inform and defect: because they are tortured, because they are induced to do so by cash, because they are blackmailed into it as the lesser of two evils, because they lose their nerve, and

Introduction: Speaking of Repression

By Kristian Williams

It is hard to talk about political repression without sounding at least a little bit paranoid. That's odd, given that the National Security Agency taps phones without court supervision, the Patriot Act gave the FBI the power to search our homes without ever notifying us, and police around the country routinely infiltrate protest groups opposed to the Iraq war. These facts—along with certain background features, like the two million Americans in prison, the existence of a concentration camp at Guantanamo Bay, and the ever-present threat of police violence—are available to anyone with access to a newspaper. Plenty of people worry about the implications for privacy, or civil liberties, or the system of checks and balances, but few seem willing to discuss the overall pattern in terms of repression.

In a way, this omission is only natural. It can be exceedingly easy to get lost in the details of this or that government program, and thus can be very difficult to relate such programs one to the other. And yet—it is almost impossible to make sense of any isolated case without some idea of the larger picture. If we want to understand what the government is up to, even at the lowest level, repression is an idea we cannot do without.

The truth is, if we view our government's activities in terms of "catching bad guys" or "making America safer" a lot of its efforts don't really make any sense. Why try to infiltrate the Quakers? Why seek out lists of participants at academic conferences? Why investigate people who write letters to the newspaper? Why bother spying on People for the Ethical Treatment of Animals when the Earth Liberation Front is burning down buildings? For that matter, why bother hunting the Earth Liberation Front when there's al Qaeda to worry about?

A great many sensible people read the headlines and just see Keystone Kops and Cold War dinosaurs wasting their own time and the taxpayers' money. What is worse, some activists deduce that the state's efforts are misguided, and therefore irrelevant, and therefore harmless—that as long as we are only involved in "peaceful dissent" we have nothing to fear from some "routine surveillance." Both assessments are mistaken, in part because they assume that the state really is in the business of catching bad guys and keeping us safe—that it only cares about violence and crime and isn't concerned with honest differences of opinion. Because these judgments misinterpret the government's aims, they cannot recognize the strategy at work.

Ken Lawrence's essay "The New State Repression" helps to elucidate that strategy—drawing the connections between police-state tactics and the government's main task, preserving the existing distribution of power. Activities that seem pointless or ineffective for crime-fighting and preserving public safety make perfect sense for tracking dissent, disrupting opposition, and controlling troublesome populations. And Lawrence doesn't just explain the strategy, he also details its development and documents the state's own analyses and self-identified objectives.

Clearly a lot has changed since 1985, when this pamphlet first appeared. The authorities are more practiced, the police are more militarized, and the technology is far more advanced. None of this renders Lawrence's essay obsolete; it shows, instead, just how well its analysis holds up, and the degree to which the strategy it outlines remains in force. "The New State Repression" shows us something of how we arrived at our current condition. And so it reminds us that repression did not begin with September Eleventh and will not go away when Bush leaves office, or when al Qaeda dissolves.

The implications here are both radical and important—not only for the activist left, but for anyone concerned with the basic principles of democracy. The ruling class and its representatives in government intend to keep their power, and they prefer to do so by *preventing* opposition rather than by defeating it. They understand potential threats not only in conspiratorial or political terms, but in sociological and economic terms as well. That is, they are not only concerned with the minorities who do oppose them, but with the majority that has reason to oppose them and so someday might. Both become targets of repression.

But the corollary is this: Our rulers need repression because they know how brittle their legitimacy really is, and how weak their grip on power. This sense of vulnerability always provides the premise for their plans, the motive for repressive action. "The New State Repression" shows us this, often from the state's perspective and largely through the words of its own strategists.

We cannot afford to underestimate the state. But we should not fool ourselves into believing in its omnipotence, either. Ken Lawrence has offered a guard against each type of error.

Kristian Williams is the author of *American Methods: Torture and the Logic of Domination* (South End Press, 2006) and *Our Enemies in Blue: Police and Power in America* (Soft Skull Press, 2004). He is a member of Rose City Copwatch, in Portland, Oregon.

military forces have begun making their appearance every time a militant anti-war protest is held anywhere in the United States.

Ironically, the strongest resistance to these developments has come from the upper echelons of the U.S. military who cling to their traditional view of their mission. They want to fight wars, not "low intensity operations." They do not want to become police. But they grudgingly obey; officers from all over the world, not just U.S. military brass, receive training in "low intensity conflict" at Fort Leavenworth's Command and General Staff College. Meanwhile, every police force worthy of the name has been thoroughly militarized with SWAT teams, tactical squads, helicopter patrols and the like.

One important difference between Kitson and Evelegh concerns the quality and importance of intelligence. Kitson says:

If it is accepted that the problem of defeating the enemy consists very largely of finding him, it is easy to recognize the paramount importance of good information.

In a lengthy chapter, he provides a long list of suggested ways to gather intelligence. One example has the policeman or soldier in charge

appoint one local inhabitant to be responsible for each street who would be instructed to appoint an individual to be responsible for each block and so on down to one individual responsible for each family.

The "beat rep" programs mentioned earlier bear a striking resemblance to this suggestion. The most significant point is so subtle that it could easily be missed, so Kitson emphasizes the point in his conclusion: *quality* of intelligence is unimportant; *quantity* is what counts.

It has already been mentioned that peace-time intelligence organizations prefer using a few high grade sources to a large number of lower grade ones. But it is evident from the scenario that the system for developing background information works if there is a lot of it to develop. It is not important that it should be immensely reliable because all that is necessary is something on which to build.

Evelegh's view is a pole apart. For him, *quality* is paramount:

lawful but as easy as possible.

Although Parliament has given the security forces draconian powers, Eveleigh wants a different emphasis, one that is often echoed in our country.

What it has not approved are measures that really would make the Security Forces more effective, but which carry a much lower political price, such as introducing identity cards or giving the soldier the right to demand the production of driving licenses and vehicle documents.

Methods currently in use in the U.S. have reduced the "political price" even further than Eveleigh envisioned. Media campaigns to frighten parents about the possibility that their children might be kidnapped are followed quickly by a concerted police/school/corporation (usually McDonald's) offer to help protect the kids by fingerprinting and photographing them; thus they are registered with the police long before they have any idea of the possible consequences. And Selective Service has purchased lists of young men who signed up long ago at an ice cream store to receive free treats on their birthdays; the government uses the lists to find 18-year-olds who haven't registered for the draft.

The United States has managed to pursue a "two track" strategy, employing both Eveleigh and Kitson's proposals simultaneously. At the same time as apparently benign Eveleigh-type policies are being implemented, such as requiring every child on welfare to have a Social Security number, the more draconian Kitson methods are also advancing, mostly under the banner of counter-terrorism.

One can marvel at the skill with which this campaign was orchestrated, from the very first days of the Reagan administration when Secretary of State-designate Alexander Haig announced the policy. Since FBI figures showed a steady decline in the number of domestic terrorist incidents, the pretext was initially international terrorism. Reports of a Libyan hit team planning to assassinate the president were widely circulated; proof that this story was a hoax received little attention. As Congress obediently furnished the money to establish the new super-secret counter-terrorist units in various branches of the military, Secretary of State George Schultz announced the government's new policy of preemptive strikes against suspected terrorists. Gradually since then, the rhetoric of government officials has obliterated any distinction between domestic and international terrorism, and strange

The New State Repression

By Ken Lawrence

Author's Introduction

(1985)

Political repression exists in three discernable forms: police brutality, which is widespread violence committed by armed agents of the state against members of oppressed communities, nationalities, and classes, usually of a diffuse and relatively random character; vigilantism, which is violence against the oppressed committed by ostensibly private (non-government) individuals and organizations, sometimes random but more typically aimed at explicit targets; and secret police activity, nearly always directed by elite government agencies against carefully chosen enemies considered to be political threats to established authority.

There is a definite relationship among these three forms of repression, and they are often employed in concert. Illegal acts of terror perpetrated by Ku Klux Klan or Nazi paramilitaries often turn out to have been planned and directed by the very law enforcement personnel who are supposed to be preventing them, and carried out against the same people deemed "subversive" by the authorities, all the while against a backdrop of escalating police brutality. It would therefore be futile to imagine struggling against one form of repression while ignoring the others.

Nevertheless, it is also necessary to understand the distinguishing features of each form of repression in order to devise adequate anti-repression strategies. For that reason, this booklet focuses mainly on the third form of repression, the activities and strategies of the secret police (the intelligence agencies), and concentrates on those aspects that are new. Readers should not interpret the restrictions on the discussion here as any sort of suggestion that the other forms of repression or the struggles against them are less important. They must be understood as clearly and fought as

vigorously as ever.

All three types of repression have undergone important changes in recent years. Police forces are not what they used to be. On the one hand, they have been militarized to a degree previously unknown in the United States; on the other hand, they are engaging in public relations campaigns to project the opposite image: the police as surrogate social workers and protectors of children. These developments, along with the introduction of "beat representatives" whose tasks range from lubricating relations between police and local businesses to low-level intelligence gathering, have necessarily changed the face of police brutality.

Racist vigilantes can no longer be safely relied on to serve as an extension of the state bringing "law and order" to areas that are difficult to govern, because they are increasingly under the sway of ideological fascists whose organizations—Ku Klux Klans, Nazis, Aryan Nations, Posse Comitatus, and many others—are in opposition to the government for their own reasons. Under these conditions, there are greater risks attached to employing these forces than in past years when such terrorists proclaimed themselves to be the most loyal Americans.

The most striking advances, however, have come in the functioning of the secret police. The resulting changes are on the most fundamental level: the way they view society and their role in it. That is our point of departure.

IV. Robin Evelegh's Alternative Strategy

Despite the widespread and continuing application of Kitson's strategy on both sides of the Atlantic, it has failed to stem the tide of insurgency in the place where it has been applied most diligently and for the longest time—Ireland—and it has suffered setbacks elsewhere. It is fitting that the person who entered the debate with the most persuasive critique and proposals to modify Kitson's basic strategy cut his teeth on the same Belfast battlefield.

Robin Evelegh has written a book which is the basis of the revised British strategy in Ireland. His approach, together with Kitson's, has become one of the standard choices available to secret police in the United States, and the issues he has raised are a matter of concern in the ongoing ruling class debate over the various methods of repression.

In *Peace-Keeping in a Democratic Society: The Lessons of Northern Ireland*, Evelegh disagrees with Kitson that the government has a choice on how to use the legal system. If the security forces are so cynical about the law that they use it purely as a device to manipulate people, they will inevitably disgrace and discredit it, and if people lose all respect for the law, all is lost, he says.

Kitson wants nearly every police activity to be conducted secretly, but Evelegh argues for openness as much as possible, so that what the police really need to do in secret they can. There's no need to skulk around in the shadows to obtain information the police can force people to provide, he reasons.

A community that does not support the Police can be policed effectively, but it is markedly different from policing a community that helps its Police. The case is therefore made for the two fundamental measures necessary to achieve detection in a population affected by terrorism. These are: to provide for the compulsory registration and identification of the population so that the Security Forces can know who is who, what they look like and where they live; and to make the active development of informers inside the terrorist ranks by the Security Forces not only

agencies.

The truth is that expansionist whites in a quest for power and wealth, largely in the name of the government, systematically annihilated thousands of Indians and claimed their heritage, the land, in the name of national progress. ... the winners incarcerated the losers and have kept them incarcerated for more than 100 years.

With the exception of the mentally deranged or the intoxicated person, all acts of illegal and criminal violence have roots somewhere in our present social, economic, or political environment.

[Our] mission can be accomplished only if we fully understand that ... legitimate violence is integral to our form of government for it is from this source that we can continue to purge our weakness ... [and] illegal violence has roots which are attached to emotional situations of political, economic, or social inequality.

It is necessary for the police executive to treat his occupation like all other executives. He must do it well but not so well that he puts himself out of a job. He must reduce crime but not stop it.

He faces an impossible task of being required by law (actually or by his own interpretation) to preserve a free and democratic society and at the same time he must eliminate crime and violence. These tasks are totally incompatible...

It is not an accident that the man who took charge of indoctrinating police with these concepts more than 15 years ago under Governor Reagan has been brought to Washington by President Reagan to carry on his work. Yet, aside from charges of misusing funds that led to a small scandal, Giuffrida has received scant scrutiny from the press, even after he made blatantly racist remarks on national television.

I. The Strategy of Permanent Repression

State repression is about as old as what people generally call civilization. Ancient Egypt had armies and police to put down Pharaoh's subjects who got uppity. Planter/General Wade Hampton led his militiamen and soldiers against the largest slave insurrection in U.S. history in 1811, in Louisiana's St. Charles and St. John the Baptist Parishes. And so on, to today. Repression isn't new, in this country or anyplace else.

But there are ways in which today's political repression differs fundamentally from the repression practiced here and around the world in the past. The most basic difference is on the level of *strategy*—not just technology, though that is important also, but the general approach of the state, the outlook of the ruling class.

In the past, the rulers and their security forces believed that the normal condition of society was stability and calm, while insurgency was thought to be a quirk, an oddity, a pathology. Certainly, they knew that rebellions would break out from time to time, and they would then have to slap them down, but only to return to "normal," where everything was quiet and peaceful.

The difference today is their belief that insurgency is not an occasional, erratic idiosyncrasy of people who are exploited or oppressed, but a constant occurrence—*permanent insurgency*, which calls for a strategy that doesn't simply rely on a police force and a national guard and an army that can be called out in an emergency, but rather a strategy of *permanent repression* as the full-time task of the security forces. This difference has been elaborated theoretically largely as a consequence of the Indochina war, which gave this strategy its name: *counterinsurgency*.

When the Black freedom movement erupted in the fifties and sixties, the state's traditional tool of repression, military violence, proved not to be as effective as in the past. The actions of Police Commissioner Eugene "Bull" Connor in Birmingham and Sheriff Jim Clark at Selma not only failed to stop the movement, they actually fanned the flames of insurgency. But as that insurgency spread to other sectors of the population, the main state

response was more of the same, culminating in the police riot in Chicago against protesters at the 1968 Democratic National Convention.

By the end of the sixties, it was clear to the ruling class that its traditional methods of social control were weakening and that its repressive apparatus was insufficient as a backup. A new approach was needed, one that started from scratch and challenged some of the bourgeoisie's most sacred beliefs about its social order. The person who answered the call was a British military commander, Brigadier Frank Kitson.

Frank Kitson's 1971 book, *Low Intensity Operations*, the basic manual of counterinsurgency in Western Europe and North America, describes insurgency as growing through three stages. The first he calls The Preparatory Period; the second, The Non-Violent Phase; the third, Insurgency.

In elaborating The Preparatory Period, Kitson describes what earlier bourgeois theoreticians would have called normality: nothing's happening, all is calm. According to Kitson, just because you can't see rebellion doesn't mean it isn't there. It really is happening. The state's enemies are gathering their forces, they're knocking on doors, they're plotting. Sooner or later they'll be out in the streets, so the police have to be ready for them. Right then, during The Preparatory Period, when nothing seems to be happening, is the time that the police must get themselves together and start penetrating the opposition, because something will develop sooner or later for sure.

That argument is a substantial departure from earlier theories of repression, and its novelty is more recent than most people might think. A few years ago, I produced a booklet about who the FBI's political targets were at different times called *J. Edgar Hoover's Detention Plan: The Politics of Repression in the United States 1939-1976*. It measured the FBI's politics of repression according to which groups Hoover had designated for internment in the event of a national emergency, a reactive model. Somebody would do something and Hoover would add them to the list. But until they actually engaged in political protest of some sort, they weren't on the list, and quite often the FBI didn't even know they existed.

That has changed. Kitson's model requires a different approach altogether. His notion is, we may not know who our enemies are, but they're out there plotting and organizing, so the police must go find them, infiltrate them, and plant provocateurs among them.

That doesn't mean they have junked everything they have done before, and some of the classical descriptions of secret police methods

The racially separated segments of our society, as they have done repeatedly in the past, have emerged with periods of sporadic violence. A white man cannot ever be black, red, or brown and so long as the white man remains superior in numbers he will be the repressor and the constant target of the mad dog.

It is in the interaction between these desperately separate segments of society—between protesters and responding authorities—which has resulted in violence. For these minority elements, any steps to prevent violence which do not address the issues of fundamental social and political change are destined to be irrelevant and fated to failure.

The single most violent force in American history, inside and outside of war, has been a small group of militant whites; ...ethnic minorities within the system become the target.

What we have discussed thus far depicts the classic struggle for social reform.

CSTI borrows from Kitson:

Most students of revolution would agree that "peaceful dissent" is the first step toward revolution and that this new trend signals the opening phases of the "new revolution."

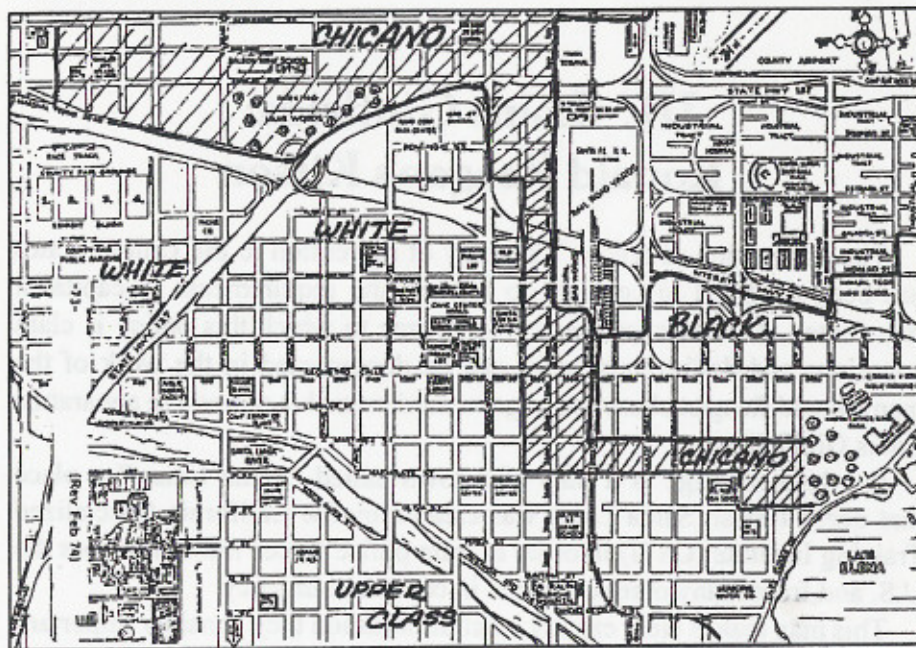
These issues, be they social, cultural, political, or economic, snowball and often appear to the casual observer as being full of truth and at least justified.

In short—it is fashionable to direct sneers, threats, and even open hostility toward the policeman. He is, symbolically at least, everything that is wrong with society.

WHEN THE NECESSARY RESPECT AND REVERENCE ARE DESTROYED, VIOLENCE, AS WE KNOW IT, WILL BE HEROISM.

[T]he remainder of our exploration on this subject will be limited to "illegal violence" directed at us, officials of responsible government

whom President Ronald Reagan appointed to head the Federal Emergency Management Agency.



The text that Giuffrida approved for CSTI's course in "Civilian Violence and Terrorism: Officer Survival and Internal Security" is one of the most revealing documents to appear since Victor Serge published the Okhrana's manual on the use of provocateurs.

Here are excerpts:

[I]t is a fact that the most powerful weapon of a revolutionary is the silent, accumulating contempt and hatred of a people directed at the government or another segment of the class structure. This thesis is magnified considerably when the chosen form of government is capitalistic and class ridden and allows for the ready labeling of all: white, black, red, brown, rich, poor, middle class, Protestant, Catholic, Jew et al.

Students in America have contributed to a long history of violence. This is not an unusual phenomenon as they, representative of each generation, are more morally and politically serious than their parents and many of their leaders.

continue to be as pertinent as ever. One of the best is Victor Serge's book, *What Everyone Should Know About State Repression*, based on the documents of the tsar's Okhrana which were captured by the Bolsheviks during the Russian Revolution. The most revealing of these documents was a manual on provocation—how the police should manage *agents provocateurs*. Nowhere has the method of employing provocateurs even been theoretically elaborated as well as in the tsarist police manual, quoted extensively in Serge's book.

Despite the promise of high technology, principally computers and electronic surveillance equipment of great sophistication, human agents remain the essential vehicle of political repression. In order not just to know what political groups are thinking and doing, but to prevent momentum from developing that would make repression much more costly, the police need people inside, not simply spying, but playing an *active* role—disrupting, discrediting, misdirecting, and neutralizing the state's opponents.

Naturally the police do apply the new technologies. They don't usually have to intercept couriers carrying messages any more; they have bugs and wiretaps and satellite surveillance, and equipment that enables them to record everything that is typed on an electric typewriter from a block away. *The Technology of Political Control* is a useful sourcebook on modern repression gadgetry; another is the collection of documents, pamphlets, and articles supplied in the United Methodist Voluntary Service packet titled *Repression and Resistance*.

But the application of any method of state repression is determined politically. The old assumption of the U.S. rulers was that the population is essentially loyal to the state, that the task was simply to identify insurgents and to expose them as disloyal. That was the method of the old House Un-American Activities Committee, the Senate Internal Security Subcommittee, Senator Joseph McCarthy, and the FBI under J. Edgar Hoover. Hoover's book *Masters of Deceit* is a classic of the genre.

These methods failed miserably in the sixties. The more they tried to "expose" the Black movement as disloyal, the larger that movement grew and the more others adopted its methods and its vision. Belatedly, the repressive agencies shifted to a different tack, mainly covert action designed to weaken the movements from within and to wage psychological warfare against them from without. The best-known examples are the FBI's Counterintelligence Program, COINTELPRO, and the CIA's domestic disruptions, Operation CHAOS and Project RESISTANCE.

For these, surveillance was not enough, no matter how sophisticated the technology. Only the presence of provocateurs within the movement could create factions and sow dissension, plant false evidence that could then be used to confuse and alienate supporters or create the basis for criminal frame-ups, and make certain that targeted leaders met their appointments with assassins' bullets. But these methods also contained risks. The types of people who can be hired to carry out these tasks are usually psychologically unstable, often drawn from the criminal element. Sometimes they "defect" to the groups they are supposed to disrupt. Sometimes they feed their employers false information in order to keep their jobs.

Kitson's approach answered some of these problems, if only because, by institutionalizing repression as a permanent feature of capitalist society, his system furnishes more opportunities for the state to recruit, place, and test its agents long before they are called upon to perform the most extreme kinds of provocations.

III. Louis Giuffrida: Ronald Reagan's Kitson

The application of Kitson's strategy of repression to the United States has been modified to conform to the specific requirements of capitalist rule rooted in white supremacy. The degree to which this policy is class conscious and deliberately racist can be documented in the work of the man Ronald Reagan chose long ago to modernize his repressive apparatus: Louis Giuffrida.

On the next page is a map of a town called "Santa Luisa," a place that doesn't exist. Santa Luisa was created by the California Specialized Training Institute (CSTI) in order to train police forces from all across the U.S. and from many other countries in counterinsurgency.

This map makes clear exactly what information they consider important for their repression plans. Trainees are given hypothetical insurgency scenarios as problems; they are then asked how they would deploy their forces in each instance. This is how counterinsurgency is actually taught and conducted.

This map shows not only the exceptional degree to which this is the conception of an imperialist power rooted in white supremacy, but also that the people who are in charge of state repression are fully aware of the basest implications of their social order. There is no pretense here that the racial and class elements are incidental; they are determining factors. It is also clear from the map and the text that accompanied it that CSTI took for granted that people of color are to be permanently oppressed and, the corollary assumption, that the Black and Latino communities will be the usual source of insurgency. The largest share of counterinsurgency planning is directed against them.

CSTI was created when Ronald Reagan was the governor of California to carry out tasks that could not, at that time, be conducted at FBI headquarters or the International Police Academy, or other federal police training institutions. But the right wing of the security establishment felt the need was urgent, so the tasks were done in California under Reagan, organized by Edwin Meese. The head of CSTI then was Louis Giuffrida,

interestingly, to spy on Vietnamese revolutionaries also, during the sixties.

One irony of Kitson's nomenclature is that during the sixties the United States government used actual street gangs, funded by the Office of Economic Opportunity, to perform some of the repressive functions assigned by Kitson to "pseudo gangs." Edward Lee's article, "The Lumpenproletariat and Repression: A Case Study," provides extensive documentation of the way this was accomplished using Blackstone Rangers in Chicago.

More recently, other organizations have played comparable roles. In the seventies, the National Caucus of Labor Committees emerged as an ostensibly Marxist organization, then began a crusade to disrupt the left with physical violence. Only later did it shed its "Marxist" garb to reveal its actual neo-Nazi politics. Another vigilante organization, the Guardian Angels, still manages to confuse some leftists as a Kitsonian "pseudo gang," even though its corporate ties and reactionary aims are known.

II. Frank Kitson in Theory and Practice

Frank Kitson was the commander of the British counterinsurgency force in the North of Ireland for many years, and before that he was an officer in many of Britain's lost colonial wars: Kenya, Aden, Cyprus. Most of his examples in *Low Intensity Operations* are drawn from Britain's war in Ireland and the U.S. war in Indochina.

He says the police and the army have to take advantage of the first stage of popular struggle, The Preparatory Period, to deploy themselves, to infiltrate the enemy. That's when people are not on their guard. That's when the cops can get their spies and provocateurs "in place" so that when open rebellion develops, as he says it must, agents are already there. Later it might be difficult or impossible to get them in.

Certain critical decisions must be made during The Preparatory Period, Kitson says:

An excellent example concerns the way the Law should work. Broadly speaking there are two possible alternatives, the first one being that the Law should be used as just another weapon in the government's arsenal, and in this case it becomes little more than a propaganda cover for the disposal of unwanted members of the public. For this to happen efficiently, the activities of legal services have to be tied into the war effort in as discreet a way as possible which, in effect, means that the member of the government responsible for the law, either sits on the supreme council or takes his orders from the head of the administration. The other alternative is that the law should remain impartial and administer the laws of the country without any direction from the government. ... As a rule the second alternative is not only morally right but also expedient because it is more compatible with the government's aim of maintaining the allegiance of the population.

Despite the disclaimer, Kitson's critics have repeatedly shown that in the counterinsurgency campaigns he himself commanded, it was always the first model that was chosen.

If the counterinsurgency war is to succeed, Kitson says the police must have a grasp of the insurgents' politics; they must sort out the different categories of enemies in order to divide and weaken them. Here is what Kitson says to do in The Non-Violent Phase, the second stage of struggle when people are leafleting and marching, but before the Insurgency begins:

For the purposes of this study no account will be taken of the simplest method of all, which is to suppress the movement by a ruthless application of naked force, because although non-violent campaigns are particularly susceptible to this sort of action, it is most unlikely that the British government, or indeed any Western government, would be politically able to operate on these lines even if it wanted to do so. In practice the most promising line of approach lies in separating the mass of those engaged in the campaign from the leadership by the judicious promise of concessions, at the same time imposing a period of calm by the use of government forces backed up by statements to the effect that most of the concessions can only be implemented once the life of the country returns to normal. Although with an eye to world opinion and to the need to retain the allegiance of the people, no more force than is necessary for containing the situation should be used, conditions can be made reasonably uncomfortable for the population as a whole, in order to provide an incentive for a return to normal life and to act as a deterrent towards a resumption of the campaign.

The raids in the Black community ostensibly searching for Assata Shakur were exactly this kind of harassment. This is an element of strategy; it is not a quirk, nor an accident, and not something to be deferred until the Insurgency begins.

The third is to associate as many prominent members of the population, especially those who have engaged in non-violent action, with the government. This last technique is known in America as co-optation.

Kitson's final stage is Insurgency. Here he says intelligence is the critical element.

If it is accepted that the problem of defeating the enemy consists very largely of finding him, it is easy to recognize the paramount importance

of good information.

Kitson's recipe calls for a technique he calls *pseudo gangs* or *counter gangs*, which he claims to have invented in Kenya during the British war against the Mau Mau. (The term itself is an excellent example of the way repressive forces attempt to criminalize their political opponents. Kitson would call any liberation movement a "gang," hence its false counterpart under police control is a "pseudo gang.")

He says it's important for these phony opposition movements to develop credibility so that they can effectively confuse, divide, and undermine the authentic organizations, and so that they can eventually serve as paramilitary auxiliaries to the security forces. He adds,

There is some evidence to the effect that pseudo-gangs of ultra-militant black nationalists are operating now in the United States.

One FBI provocateur based in Tampa, Florida named Joe Burton created organizations all over the United States and Canada between 1972 and 1975. His home base group in Tampa was called Red Star Cadre. Most of its far-flung affiliates, but not all, presented themselves as Maoist: some were ostensibly pro-Soviet or pro-Cuba. The FBI used these front groups sometimes to disrupt legitimate revolutionary movements in the U.S., other times to unify with and spy on them.

One of the things his career teaches us is the political sophistication of the FBI. An FBI control agent would fly down to Tampa from Chicago to help Burton compose his political literature so its political line would closely match the line of the target organization, in order to achieve the credibility Kitson considers so important. Sometimes it was Maoist, sometimes Fidelista, and so forth.

That was when the purpose was to spy. Disruption operations were handled differently. When Burton's assignment was to interfere with the United Electrical, Radio and Machine Workers of America's attempt to organize a union at the Westinghouse plant in Tampa, he attacked everyone: they were all denounced as "revisionists" no matter what their political lines happened to be. This versatility and familiarity with the minutiae of Marxist doctrine exhibits a degree of political sophistication that we do not often associate with the security forces.

Another example was a bogus Black liberation organization in St. Louis which the FBI used to misdirect other Black organizations in the U.S. and,

The Other Side of the COIN:

Counterinsurgency and Community Policing¹

DRAFT VERSION: NOT FOR CIRCULATION OUTSIDE BTR

Kristian Williams

Introduction: Expect Repression

Oppositional political movements inevitably face -- and therefore ought to expect -- repression at the hands of the state. But, while quick to condemn the most obvious and violent manifestations of state repression, especially when directed against peaceful groups, the left has been slow to grasp the strategy underlying the state's approach.

We tend to characterize repression as the state's response to crisis, rather than seeing it also as a means to preserving normalcy. Hence, it has been very difficult to recognize it in quiet times, and when it does appear it seems like an exception, an excess, a panicked over-reaction.

But repression does not always come dressed up in riot gear, or breaking into offices in the middle of the night. It also comes in the form of the friendly “neighborhood liaison” officer, the minority advisory boards to local police departments, and the social scientist hired on as a consultant. Repression is, first and foremost, a matter of *politics*: it is the means the state uses to protect itself from political challenges, the methods it employs to preserve its authority and continue its rule. This process does not solely rely on force, but also mobilizes ideology, material incentives, and, in short, all of the tools and techniques of statecraft. So we have to understand repression as involving both coercion and concessions, employing violence and building support, weeding opposition and seeding legitimacy. That is the basis of the counterinsurgency approach.

¹ This paper grew out of a lecture presented at the "Econvergence," First Unitarian Church, Portland Oregon; October 3, 2009. Thanks are owed to those who offered comments on that talk, and on my later presentation at the National Lawyers Guild Northwest Regional Conference (Lewis and Clark Law School, Portland, Oregon; April 17, 2010). Also, I am grateful to the numerous people who offered detailed comments on earlier drafts, in particular: Jules Boykoff, Emily-Jane Dawson, Colette G., Don H., Chris Knudtsen, Peter Little, Geoff McNamara, Will Munger, Steve Niva, Janeen P., Josef Schneider, M. Treloar, and Kevin Van Meter.

This essay outlines the counterinsurgency model ("COIN" in the military jargon), with an emphasis on its domestic application. It shows that, despite the term's association with colonialism and Latin American "dirty wars," many contemporary counterinsurgency practices were developed by police agencies inside the United States and continue to be used against the domestic population.

The argument proceeds through four stages. Part one describes the counterinsurgency approach as it is presented in military documents and the professional literature, especially the U.S. Army Counterinsurgency Field Manual (FM 3-24), and recent studies produced by the Rand Corporation.² The second part illustrates the transfer of COIN theory, strategy, technique, and personnel from the military sphere to the domestic policing context, and *vice versa*. The third explains the state's use non-governmental or non-profit agencies, alongside military and police action, to channel and control opposition. And finally, the conclusion considers some implications for social movements, in particular those of the left, in their efforts to overcome repression and achieve political change.

In this context, the title -- "The Other Side of the COIN" -- has three distinct meanings, which correspond with the main themes of my argument. First, it refers to the strategic pairing of direct coercion and subtle legitimacy-building activities. Second, it points to the joint development of military operations overseas and police control domestically. And third, it reminds us that when the authorities turn to counterinsurgency it's because they fear that insurgency is brewing. Wars -- especially revolutionary wars -- have two sides.

The state, at least, understands that there is a war underway. It is time that the left learns to see it.

² The Rand Corporation, founded in 1948, serves as an independent think tank for the Defense Department.

It's important to recognize the limits of the official documents. What I am describing here is the theory of counterinsurgency, not a set of hard and fast rules. The practice of COIN often diverges from the doctrine, and sometimes diverges very sharply. To some degree this is inherent in the dynamic, localized nature of counterinsurgency warfare, and a lot (as always) depends on the judgment of commanders on the ground. Imperfect adherence to the counterinsurgency model may indicate institutional inertia, internal disagreements, inter- or intra-agency rivalry, limits of capacity and competence, a lack of political will, or any number of other real-world operational or organizational factors. But it may also point to the ideological constraints shaping the guiding documents. Admonishments to operate within the law and to demonstrate a respect for human rights, for example, are compulsory in official publications and should be met with considerable skepticism.

Part One: Repression, Counterinsurgency, and the State

Some Definitions

One of my objectives in this paper is to broaden and deepen our understanding of repression. I hope to show how repression functions in the course of the normal operations of the liberal state, and to demonstrate its effects in contexts that are not usually thought of as repressive, or even as necessarily political. At the same time, however, I am not seeking to redefine the word, but simply to apply the standard definitions with greater consistency; so I am employing the word "repression" in its usual political sense, referring to the "process by which those in power try to keep themselves in power by consciously attempting to destroy or render harmless organizations and ideologies that threaten their power."³

"Counterinsurgency," is not simply synonymous with "repression," but has a narrow, technical meaning, which of course relies on the definition of "insurgency." U.S. Army Field Manual 3-24, *Counterinsurgency*, explains:

"[An] insurgency [is] an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict. .

..

Stated another way, an insurgency is an organized, protracted politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control."

The definition of counterinsurgency logically follows: "Counterinsurgency is military, paramilitary, political, economic, psychological, and civic actions taken by a

³ Alan Wolfe, *The Seamy Side of Democracy: Repression in America* (Reading, MA: Longman, 1978), 6.

I focus here on state repression, though of course other powerful actors engage in repressive activities as well. For example, *The Nation* reports that the mercenary firm Blackwater offered to infiltrate animal rights groups on behalf of the genetic-engineering behemoth Monsanto. Jeremy Scahill, "Blackwater's Black Ops," *The Nation*, October 4, 2010.

government to defeat insurgency." The two concepts operate together, describing opposing forces: "insurgency and COIN are two sides of a phenomenon that has been called revolutionary war. . . ."4

Insurgents are the revolutionaries; counter-insurgents are the counter-revolutionaries. The insurgents do what they can to shift power away from the state and toward the social movement of which they are a part. The counter-insurgents, likewise, use all available means to preserve the state's power.

Ends and Means

"Counterinsurgency," then, refers to both a type of war and a style of warfare. The term describes a kind of military operation outside of conventional army-vs.-army war-fighting. It is sometimes called "low-intensity" or "asymmetrical" combat, and is linked conceptually to nation-building. But counterinsurgency also describes a particular perspective on *how* such operations ought to be managed. This style of warfare is characterized by an emphasis on intelligence, security and peace-keeping operations, population control, propaganda, and efforts to gain the trust of the people.⁵

This last point is the crucial one. As FM 3-24 declares: "*Legitimacy is the main objective.*" It goes on to explain:

"All governments rule through a combination of consent and coercion. Governments described as 'legitimate' rule primarily with the consent of the governed. . . . [The government] still uses coercion—for example, against criminals—but most of its citizens voluntarily accept its governance."⁶

The primary aim of counterinsurgency is political.⁷ That's why, in the context of the American occupation of Iraq, we heard career officers arguing that "victory in combat

⁴ Field Manual 3-24, *Counterinsurgency* (Department of the Army, December 2006), 1-2.

⁵ See, for example, FM 3-24, Table 1-1, "Successful and Unsuccessful Counterinsurgency Operational Practices."

⁶ FM 3-24, 1-113, emphasis in original.

⁷ David Galula, *Counter-Insurgency Warfare: Theory and Practice* (New York: Frederick A. Praeger, 1965) 89.

is only a penultimate step in the larger task of 'winning the peace'."⁸ And it's the need for legitimacy that they're referring to when they say that "Military action is necessary . . . but it is not sufficient. There needs to be a political aspect."⁹

The political ends rely in large part on political means. As David Gompert and John Gordon write, in the Rand Corporation's definitive report on the subject:

"In COIN, the outcomes are decided mainly in the human dimension, by the contested population, and the capabilities of opposing armed forces are only one factor in determining those outcomes. The people will decide whether the state or the insurgents offer a better future, and to a large extent which of the two will be given the chance."¹⁰

The Rand report is titled, appropriately, *War by Other Means*. War, as Clausewitz observed, is politics by other means. And politics, as Foucault reasoned, is war by other means.¹¹ But in counterinsurgency, the means are not so "other." War-fighting and state-building turn out to be very much the same exercise, as both are characterized by the effort to establish legitimacy, control territory, and monopolize violence.

The aims of counterinsurgency thus correspond almost exactly to the main characteristics of a state. As Weber defined it,

"the state is the form of human community that (successfully) lays claim to the *monopoly of legitimate physical violence* within a particular territory. . . . [O]ther organizations or individuals can assert the right to use physical violence only insofar as the *state* permits them to do so. The

⁸ Justin Gage, *et al.*, "Winning the Peace in Iraq: Confronting America's Informational and Doctrinal Handicaps," (Norfolk, Virginia: Joint Forces Staff College; Joint Combined Warfighting School, Intermediate Class 03-3, September 5, 2003) 1.

⁹ General David Petraeus. Quoted in "General Says Iraq Talks Critical." *BBC News*. March 8, 2007. <http://news.bbc.co.uk/2/hi/6429519.stm>.

¹⁰ David C. Gompert and John Gordon IV, *et al.*, *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency* (Santa Monica: Rand, 2008) 76.

¹¹ For Foucault's discussion of Clausewitz's aphorism, and his own inversion of it, see: Michel Foucault, "Society Must Be Defended": *Lectures at the Collège de France, 1975-76*," eds. Mauro Bertani and Alessandro Fontana, trans. David Macey (New York: Picador, 2003) 15-6.

state is regarded as the sole source of the 'right' to use violence."¹²

Counterinsurgency is all about preserving (or re-establishing) the state's authority. Violence and territory are inherent to the project, but it is really legitimacy -- "the consent of the governed," "societal support"¹³ -- that separates the winners from the losers. Overwhelming might is not enough, and militarily weak but politically popular movements can defeat militarily superior but politically unpopular states. That's why the U.S. lost the war in Vietnam, for example -- and why it may still lose in Iraq and Afghanistan:

"If COIN were just a form of combat the superior forces of governments and their supporters would win more often than they do. On average, insurgencies that are outnumbered and outgunned by COIN military forces nevertheless prevail if they enjoy greater popularity than the authoritarian, incompetent, or greedy governments they mean to oust."¹⁴

As Gompert and Gordon put it: "The key in COIN is not to monopolize force but to monopolize *legitimate* force."¹⁵

Theories of Repression: GWOT vs. COIN

It is for these reasons that the Rand researchers -- hardly known for their dovish or progressive ideology -- argue that, conceptually, the "War on Terror" has been a mistake: first, because it identified "terror" as the problem; and second, because it proposed "war" as the solution.

"The idea of GWOT [the Global War on Terror] . . . has fixed official U.S. attention on terrorists, with insufficient regard for the hostility that exists among

¹² Max Weber, "Politics as a Vocation," in *The Vocation Lectures*, ed. David Owen and Tracy B. Strong, trans. Rodney Livingstone (Indianapolis: Hackett Publishing Company, 2004) 33, emphasis in original.

¹³ FM 3-24, 1-113 and 1-115.

¹⁴ Gompert and Gordon, *War by Other Means*, 35. See also: CIA 8.

¹⁵ Gompert and Gordon, *War by Other Means*, xxxvii.

vastly larger numbers of Muslims. . . . The indelible image of jihadists scheming alone in remote mountain caves is less the reality of Islamic insurgency than is far larger numbers of jihadists moving freely among Muslim populations. . . . [T]error inspired by Islamic extremism is part of a larger pattern of Muslim 'resistance' that has significant popular appeal. . . . [Therefore,] terrorism cannot be defeated unless the insurgencies in which it is embedded are successfully countered."¹⁶

Thus, the solution requires, not just military might, but "intelligence, political action, civil assistance, and other nonmilitary means that might curb Islamic militancy more effectively and at less cost and risk" than simple combat.¹⁷

It seems that the U.S. is slowly re-learning the lessons of the British colonial wars.

Stages of Insurgency

In 1971 British brigadier Frank Kitson looked back on his efforts at holding the empire together in places like Kenya, Cypress, and Northern Ireland. He systemized his approach in a book titled *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*. It remains one of the most insightful books on the dynamics of revolutionary and counter-revolutionary warfare. In it, Kitson observed:

"Looking in retrospect at any counter-subversion or counter-insurgency campaign, it is easy to see that the first step should have been to prevent the enemy from gaining an ascendancy over the civil population, and in particular to disrupt his efforts at establishing his political organization. In practice this is difficult to achieve because for a long time the government may be unaware that a significant threat exists, and in any case in a so-called free country it is regarded as the opposite of freedom to restrain the spread of a political idea."¹⁸

¹⁶ Gompert and Gordon, *War by Other Means*, 6-8.

¹⁷ Gompert and Gordon, *War by Other Means*, 7.

¹⁸ Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping* (Hamden, Connecticut: Archon Books, 1971) 67.

Concerns with liberty aside, that is exactly what Kitson recommended -- government action to restrict the spread of ideas, prevent radicals from achieving public influence, and disrupt their efforts to establish oppositional organizations.

War by Other Means offers a similar analysis. According to Gompert and Gordon, revolutions (and thus counter-revolutions) go through three stages: a proto-insurgency, a small-scale insurgency, and major insurgency. At first, in the "*proto-insurgency* stage" the movement is

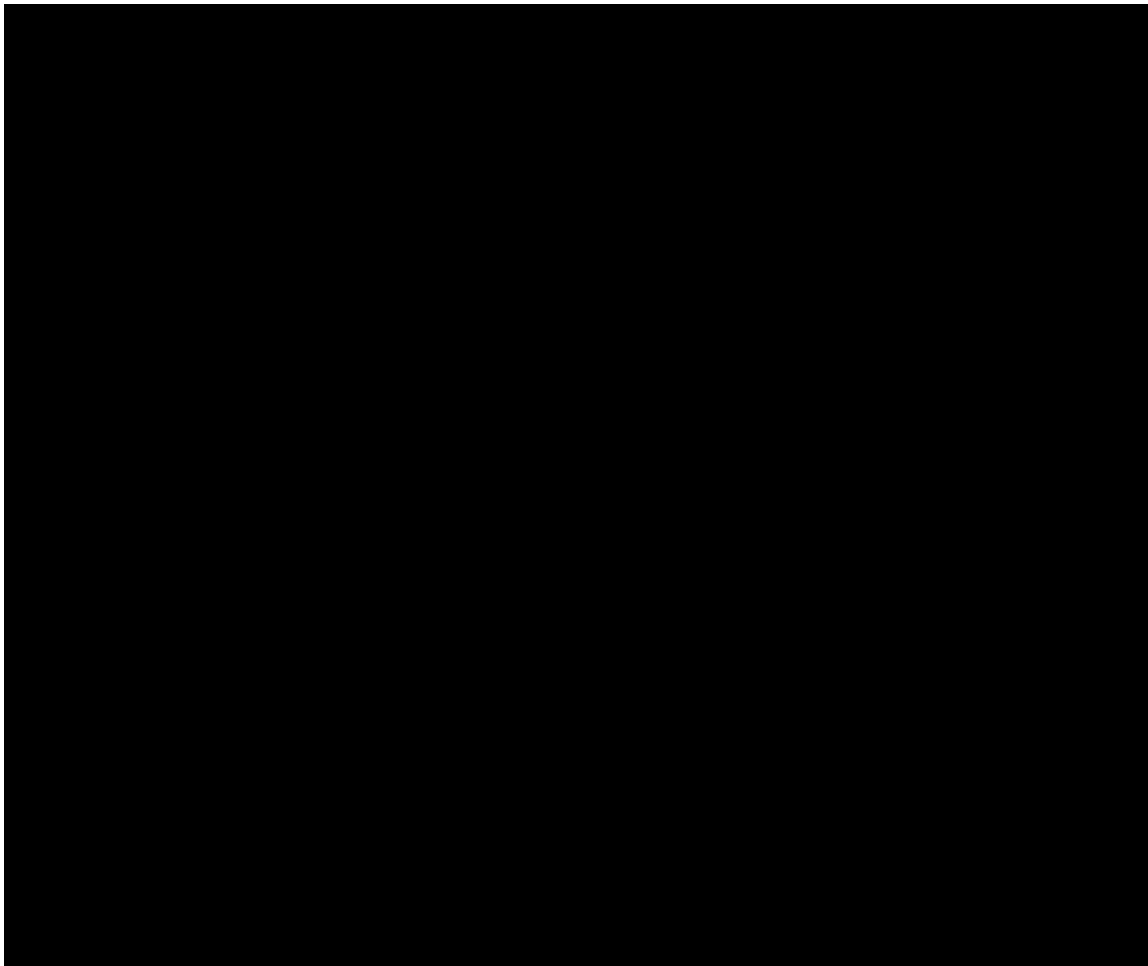
"small, narrowly based, vulnerable, and incapable of widespread or large-scale violence. Proto-insurgents may be barely noticeable, not seen as having the potential to inspire insurgency, or dismissed as criminals or inconsequential crack-pots. Therefore, during proto-insurgency, the most important aspect of COIN is to understand the group, its goals, its ability to tap popular grievances, and its potential. In turn, shaping the proto-insurgency's environment, especially by improving governance in the eyes of the population, may deny it wider support. . . ."

In the second stage, as "*a small-scale insurgency*" the movement begins "attracting followers beyond its original cadre," and it may "commit more daring and destructive acts against the state, not (yet) with a view toward replacing it, but to demonstrate its capabilities, be taken seriously by the population, and recruit." For the government, therefore, "shaping political and economic conditions to head off popular support for the insurgency is imperative." Direct military intervention is *not* recommended: "As long as the insurgency is still small, action against it can and should remain a police and intelligence responsibility."

If the movement survives, it may develop into a "*major insurgency*." While it is still "essential" that the state gain information on the movement and intervene to shape social conditions, at this stage, "forceful action against the insurgents by regular military units may be unavoidable." But again, military action, on its own, will not be sufficient. "Whether the use of military forces in COIN leads to success,

stalemate, or stronger and bolder insurgency depends on the legitimacy and skill of the state and its forces."¹⁹

To illustrate this progression, the report provides the following diagram:²⁰



Rand advocates early, preemptive action short of direct military force. The problem, as Kitson rightly noted, is that at the first stage, subversion is not obvious and the state may not know that a threat exists. Worse, the real threat must be understood as extending beyond the insurgents themselves -- the militants, radicals, and subversives -- and beyond even their base of support, to include the grievances they seek to address and the social conditions that produce those grievances.

¹⁹ The report also considers a final possibility -- *foreign military intervention*. Gompert and Gordon, *War by Other Means*, 36-7, emphasis added.

²⁰ Gompert and Gordon, *War by Other Means*, Figure 2.2, "Life-Cycle of Insurgency and COIN."

The Social Science of Repression

To meet the challenges of counterinsurgency, the security forces have had to shift their understanding of intelligence.

Since the cause of the conflict is not just a subversive conspiracy, but necessarily connects to the broader features of society, the state agents cannot simply ferret out the active conspirators, but need to aim at a broad understanding of the social system. The U.S. Army Field Manual on Counterinsurgency, FM 3-24, incorporates this perspective:

"Intelligence in COIN is about people. U.S. forces must understand the people of the host nation, the insurgents, and the host-nation (HN) government. Commanders and planners require insight into cultures, perceptions, values, beliefs, interests and decision-making processes of individuals and groups. These requirements are the basis for [data] collection and analytical efforts."²¹

Similar lists of intelligence requirements appear in the Special Forces manual on *Foreign Internal Defense* (FM 31-20-3) and the CIA's *Guide to Analysis of Insurgency*.²²

These are sociological questions. And so, a great deal of FM 3-24 is devoted to explicating basic social-science terms like "group," "coercive force," and "social capital." In fact, the entirety of Appendix B is devoted to explaining "Social Network Analysis and Other Analytic Tools." It offers this picture of how such analysis is practiced:

"[A] social network is not just a description of who is in the insurgent organization; it is a picture of the population, how it is put together and how members interact with one another. . . .

To draw an accurate picture of a network, units need to identify ties among its members. Strong bonds formed over time by family, friendship, or organizational association characterize these ties. Units gather information on

²¹ FM 3-24, 3-2.

²² Field Manual 31-20-3, *Foreign Internal Defense Tactics, Techniques, and Procedures for Special Forces* (Washington, D.C.: Department of the Army, September 20, 1994) 1-3 to 1-6; and, [Central Intelligence Agency], *Guide to Analysis of Insurgency* [no date].

these ties by analyzing historical documents and records, interviewing individuals, and studying photos and books. . . . Charts and diagrams lead to understanding the insurgents' means of operations. These same diagrams are also useful for understanding tribal, family, NGO [Non-Governmental Organization], and transnational terrorist elements. Each diagram and chart may have links to another or several others, but they are not created overnight. It takes time, patience, detailed patrolling, and reporting and recording of efforts."²³

The security forces can no longer focus narrowly on the hunt for subversives or terrorists, but must also collect information on the population as a whole. This changes, not only the *type* of information they're seeking, but also, therefore, the *means* they use to collect it. As *Byting Back*, a Rand report on information warfare in counterinsurgency, emphasizes:

"Even during a security operation, the information needed for counterinsurgency is as much or more about context, population, and perceptions as it is about the hostile force. . . . [O]nly a small fraction of the information needed would likely be secret information gathered by secret means from secret sources."²⁴

With this in mind, the report suggests a few specific mechanisms for collecting broad-based information: tracking cell phone use, conducting a national registry-census, installing vehicle- and weapon-mounted video cameras, and analyzing internet sites (in particular, creating a "national Wiki (where citizens describe their community).")²⁵

Intelligence and Coercion

²³ FM 3-24, B-47 and B-49.

²⁴ Martin C. Libicki, *et al.*, *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents* (Santa Monica: Rand, 2007) 133.

²⁵ Libicki, *Byting Back*, 9.

"Why collect such information?" the Rand researchers ask.

The answer they provide is quite revealing. The information the state acquires can be used in five types of activity: (1) police and military operations "such as sweeps, roadblocks, or arrests"; (2) assessments of progress in the counterinsurgency campaign ("How many people have been hurt or killed in the war; what kind of crimes are being committed; who is getting employment and where; and who is staying put or leaving the country?"); (3) "the provision of public services, whether security and safety services (e.g., an efficient 911 system) or social services (e.g., health care, education, and public assistance)"; (4) identifying insurgents ("distinguish[ing] those willing to help from those eager to hurt"); and, (5) the coercion of individuals for purposes of winning cooperation and recruiting informants.

This last point shows something of the relationship between intelligence and coercion, and the ways each can feed the other: "[To] be somewhat indelicate," the Rand team writes, "information about individuals may be necessary to persuade each one to help the government rather than helping the insurgents." That's because both sides rely on the cooperation of the populace:

"Insurgencies are defeated, in large part, by intelligence, much of which comes from the citizenry: e.g., witnesses to events or intelligence about who is affiliated with whom. Insurgents, in turn, want to know who is informing on *them* or at least who is cooperating or working with the government in general."

The two sides, therefore, compete for this cooperation, in part through coercive -- sometimes terrorist -- means: "Those uncommitted to either side should weigh the possibility that the act of informing or even interacting with one side may bring down the wrath of the other side." Whoever is best able to make good on this threat will, by this theory, receive the public's cooperation and will therefore also have the best information: "The balance of coercion dictates the balance of intelligence."²⁶ And, of course, the better the intelligence, the more effective the use of force can be.

²⁶ Libicki, *Byting Back*, 21-3 emphasis in original.

In short: The purpose of identifying the insurgent network is to disrupt it. And the point of understanding the population is to control it.

As we shall see, the same logic applies domestically.

Part Two: Cops and COIN

The Community Policing Paradigm

In my book *Our Enemies in Blue*, I devoted an entire chapter to the argument that the two major developments in American policing since the 1960s – militarization and community policing – are actually two aspects of a domestic counterinsurgency initiative. I summed up the idea with a simple equation: “Community Policing + Militarization = Counterinsurgency.”²⁷

In the last few years, the counterinsurgency literature has become increasingly explicit on this point. For example, *War by Other Means* lists, among the law enforcement “capabilities . . . considered to be high priority” in COIN: “well-trained and well-led community police and quick-response, light-combat-capable (constabulary) police.”²⁸ Similarly, a Joint Special Operations University report, *Policing and Law Enforcement in COIN: The Thick Blue Line*, purports:

“The predominant ways of utilizing police and law enforcement within a COIN strategy . . . consist of the adoption of the community-policing approach supported by offensive-policing actions such as paramilitary operations, counterguerrilla patrolling, pseudo operations [in which state forces pose as insurgent groups], and raids.”²⁹

²⁷ Kristian Williams, *Our Enemies in Blue: Police and Power in America* (Brooklyn: Soft Skull Press, 2004) 255.

For my full analysis of the relationship between militarization and community policing, and for my complete list of sources, see chapter 9, “Your Friendly Neighborhood Police State.”

²⁸ Gompert and Gordon, *War by Other Means*, xlv.

²⁹ Joseph D. Celeski, *Policing and Law Enforcement in COIN: Thick Blue Line* (Hulbert Field, Florida: The JSOU Press, 2009) 40.

Concerning the use of pseudo-ops, see: Lawrence E. Cline, *Pseudo Operations and Counterinsurgency: Lessons from Other Countries* (Carlisle, Pennsylvania: U.S. Army War College, Strategic Studies Institute, June 2005) 1.

Though the public generally misunderstands the relationship between militarization and community policing, the advantages the state receives from each are fairly clear: Militarization obviously increases available force, but as important, it also provides increased discipline and command and control. It re-orders the police agency to allow for better coordination and teamwork, while also opening space for local initiative and officer discretion. Community policing, meanwhile, helps to legitimize police efforts by presenting cops as problem-solvers. It forms police-driven partnerships that put additional resources at their disposal and co-opt community leadership. And, by increasing daily, friendly contacts with people in the neighborhood, community policing provides a direct supply of low-level information.³⁰ These are not incidental features of community policing programs; these aspects speak to the real purpose.

In fact, Rand goes so far as to present community policing as its *paradigm* for counterinsurgency:

"[P]acification is best thought of as a massively enhanced version of the 'community policing' technique that emerged in the 1970s. . . . Community policing is centered on a broad concept of problem solving by law enforcement officers working in an area that is well-defined and limited in scale, with sensitivity to geographic, ethnic, and other boundaries. Patrol officers form a bond of trust with local residents, who get to know them as more than a uniform. The police work with local groups, businesses, churches, and the like to address the concerns and problems of the neighborhood. Pacification is simply an expansion of this concept to include greater development and security assistance."³¹

The military's use of police theory -- in particular the adoption of a "community policing" perspective -- shows something of the cyclical exchange between the various parts of the national security apparatus.

³⁰ William Rosenau, *Subversion and Insurgency* (Santa Monica: Rand, 2007) 15.

³¹ Austin Long, *On Other War: Lessons from Five Decades of RAND Counterinsurgency Research* (Santa Monica: Rand, 2006) 53.

The Cycle of Violence: Imports and Exports

Domestically, the unrest of the 1960s left the police in a difficult position. The cops' response to the social movements of the day -- the civil rights and anti-war movements especially -- had cost them dearly in terms of public credibility, elite support, and officer morale. Frequent and overt recourse to violence, combined with covert (often illegal) surveillance, infiltration, and disruption, had not only failed to squelch the popular movements, it had also diminished trust in law enforcement.

The police needed to re-invent themselves. Practically the first place they looked for models was the military.³² The birth of the paramilitary unit -- the SWAT team -- was one result.³³ A new, more restrained, crowd control strategy was another.³⁴ Military training, tactics, equipment, and weaponry, made their way into domestic police departments -- as did veterans returning from Vietnam, and, more subtly, military approaches to organization, deployment, and command and control. Police strategists specifically began studying counterinsurgency and counter-guerilla warfare.³⁵

At the same time, and seemingly incongruously, police were also beginning to experiment with a "softer," more friendly type of law enforcement -- foot patrols, neighborhood meetings, police-sponsored youth activities, and attention to quality-of-life issues quite apart from crime.³⁶ A few radical criminologists saw this for what it was -- a domestic "hearts and minds" campaign. The seminal study *The Iron Fist and the Velvet Glove* described it as "The Pacification Model".³⁷

"[We] think that it's useful to regard the new approach to the police as

³² Christian Parenti, *Lockdown America: Police and Prisons in the Age of Crisis* (London: Verso, 1999) 25.

³³ Research on Criminal Justice, *The Iron Fist and the Velvet Glove: An Analysis of the U.S. Police* (Berkeley, California: Center for Research on Criminal Justice, 1975) 48-50.

³⁴ See: Williams, *Our Enemies in Blue*, 220-22. Also: Clark McPhail, *et al.*, "Policing Protest in the United States: 1960-1995," in *Policing Protest: The Control of Mass Demonstrations in Western Democracies* (Minneapolis: University of Minnesota Press, 1998).

³⁵ Daryl F. Gates (with Diane K. Shah), *Chief: My Life in the LAPD* (New York: Bantam Books, 1992) 109; and, Ken Lawrence, *The New State Repression* (Portland, Oregon: Tarantula, 2006) 13-16.

³⁶ *Weed and Seed Implementation Manual* (Washington, D.C.: U.S. Department of Justice, August 2005) 65.

³⁷ Center for Research on Criminal Justice, *The Iron Fist and the Velvet Glove*, 54.

having two distinct but closely related sides. One is a 'hard' side, based on sophisticated technology and a generally increased capacity to use force; the other is a 'soft' side, based on new forms of community pacification and other attempts to 'sell' the police to the public. . . .

It's important to recognize that both sides of the new police approach are strategies of repression. . . . Like the similar techniques developed in the sixties to maintain the overseas empire (on which many of the new police techniques were patterned), these new police strategies represent an attempt to streamline and mystify the repressive power of the state, not to minimize it or change its direction. The forms of repression may change, but their functions remain the same."³⁸

Both militarization and community policing arose at the same time, and in response to the same social pressures. And, whereas the military largely neglected COIN in the post-Nam era,³⁹ the police kept practicing, and developing, its techniques -- so that, when facing insurgencies in Iraq and Afghanistan, the military turned to police for ideas.

The lines of influence move in both directions.

Statistical Control

Among the police innovations that COIN theorists recommend for military use are: the Neighborhood Watch,⁴⁰ embedded video,⁴¹ and the use of computerized intelligence files,⁴² and statistical analysis. The last pair are particularly interesting.

In *Byting Back*, Martin Libicki explains the utility of statistical analysis programs, with domestic examples:

³⁸ Center for Research on Criminal Justice, *The Iron Fist and the Velvet Glove*, 30.

³⁹ Long, *On Other War*, 9; Jason H. Beers, *Community-Oriented Policing and Counterinsurgency: A Conceptual Model* (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 2007) 2; and Christopher Paul, *et al.*, *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency* (Santa Monica: Rand, 2010) xiii.

⁴⁰ Celeski, *Policing and Law Enforcement in COIN*, 43

⁴¹ Libicki, *Byting Back*, 79-80.

⁴² Gary D. Calese, *Law Enforcement Methods for Counterinsurgency Operations* (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, School of Advanced Military Studies, 2004) 41-2.

"Incidents data are, or should be, the province of security officials. . . . Such incidents would range from visible crimes, to crime reports, and nonroutine contacts between citizens and authorities. What gets included need not be incidents as such -- odd behavior may suffice. This amalgamation can be a quite valuable tool. COMPSTAT (computerized statistics), New York City's master compilation of crime reports, for instance, deserves a chunk of the credit for the city's falling crime rate in the 1990s."⁴³

Though its effect on actual *crime* is debatable,⁴⁴ Compstat certainly served as the organizational keystone for the NYPD's city-wide crackdown during the Giuliani years. It enabled police administrators to identify high-crime areas, deploy their officers strategically, and measure the progress of their efforts. Since that time, other departments around the country have adopted similar systems.⁴⁵

Byting Back notes:

"Many police departments (*e.g.*, in Chicago or Los Angeles) make it a point for officers to make systematic notes of street behavior (especially when it may involve gangs). Officers receive a specific list of what to look for. Such notes are collected, processed into a database, and made available throughout the police department."⁴⁶

The Los Angeles system was proposed by LAPD Sgt. Shannon Paulson, a Navy intelligence reservist, and implemented under Chief William Bratton, who also introduced the Compstat program in New York.⁴⁷ In L.A., street cops carry a checklist of

⁴³ Libicki, *Byting Back*, 25.

⁴⁴ See, for example: James Lardner, "Can You Believe the New York Miracle?" *New York Review of Books*, August 14, 1997; and, Sidney L. Harring and Gerda W. Ray, "Policing a Class Society: New York City in the 1990s," *Social Justice* (Summer 1999).

⁴⁵ Parenti, *Lockdown America*, 75-6 and 83-9.

⁴⁶ Libicki, *Byting Back*, 25.

⁴⁷ Siobhan Gorman, "LAPD Terror-Tip Plan May Serve as Model," *Wall Street Journal*, April 15, 2008; Josh Meyer, "LAPD Leads the Way in Local Counter-Terrorism," *Los Angeles Times*, April 14, 2008.

65 "suspicious activities" and are required to file reports whenever they see them, even if no crime has been committed. Included on the list are behaviors such as: taking measurements, using binoculars, taking photos "with no apparent esthetic value," drawing diagrams, making notes, and expressing extremist views.⁴⁸ The "Suspicious Activity Reports" are then be routed through the nearest "fusion center," the Joint Regional Intelligence Center, where they can be compiled, analyzed, and shared with other agencies -- including local and national law enforcement agencies, the military, private corporations, and possibly, foreign governments.⁴⁹ The LAPD, along with the U.S. Directorate of National Intelligence, are hoping to replicate this system in 62 other cities around the country, beginning with Boston, Chicago, and Miami.⁵⁰

Biometric Identification

Similarly, networked computer files are being used by the military to identify and track insurgents: The Biometric Automated Toolkit (BAT) has been used in both Iraq and Afghanistan to compile databases of residents, detainees, and resistance fighters. Late in 2004, following the siege of Fallujah, the city's entire population was fingerprinted, retina-scanned, and issued ID cards required for travel or to receive government services. Since 2007, similar biometric readers were used at military checkpoints in Baghdad to control movement between ethnic enclaves.⁵¹

Another program, dubbed "Snake Eater," is a variation of the system originally developed for use by the Chicago Police; it "has been adapted by Lockheed-Martin for the U.S. Marines in Anbar province, apparently to good effect."⁵² The Snake Eater kit includes mobile fingerprint, iris, and retina scanners, a digital camera, a GPS system, and a laptop computer capable of linking to a database of the local population. In the future, it is hoped the system will access the FBI's biometric database as well.⁵³

⁴⁸ Mike German and Jay Stanley, "Fusion Center Update," (American Civil Liberties Union, July 2008) 2.

⁴⁹ Michael German and Jay Stanley, "What's Wrong with Fusion Centers?" (New York: American Civil Liberties Union, December 2007) 12 and 14-5; Gorman, "LAPD Terror-Tip Plan."

⁵⁰ Meyer, "LAPD Leads the Way"; Gorman, "LAPD Terror-Tip Plan."

⁵¹ Stephen Graham, *Cities Under Siege: The New Military Urbanism* (London: Verso, 2010) 129.

⁵² Libicki, *Byting Back*, 25.

⁵³ Roberto Gonzalez, *American Counterinsurgency: Human Science and the Human Terrain* (Chicago: Prickly Paradigm Press, 2009) 90-1.

Of course, the military has been preparing for this sort of operation for a long time: 1999's "Urban Warrior" training exercises included the biometric scanning of "resistance fighters" -- in Oakland, California.⁵⁴

Gang Wars: From California to Afghanistan

A decade after Urban Warrior, marines were still refining their skills in California's cities. In the summer of 2010, seventy marines from Camp Pendleton spent a week accompanying Los Angeles police, in preparation for deployment to Afghanistan. The marines wanted to learn the basics of anti-gang investigations, standards of police professionalism, and techniques for building rapport with the community. Once deployed, the troops will pass that knowledge on to the new Afghan police.⁵⁵

Another marine, Captain Scott Cuomo, trained with the LAPD countergang unit earlier in the year. A *New York Times* profile of Captain Cuomo gives some idea of what he learned, and how he applied it in Afghanistan:

"The same Marines patrolled in the same villages each day, getting to recognize the residents. They awarded the elders construction projects and over hours of tea drinking showed them photographs they had taken of virtually every grown male in their battle space. 'Is this guy Taliban?' the Marines asked repeatedly, then poured what they learned into a computer database."

After a couple months, their efforts paid off. A villager identified a suspect, and the marines raided his house, arresting him and seizing weapons and opium. They placed the man, Juma Khan, in "a holding pen the size of a large dog cage" and interrogated him for

It is interesting to recall, in this context, that the introduction of computerized records in was itself initially regarded as a step in the *militarization of policing*. See, for example: Kevin D. Haggerty and Richard V. Ericson, "The Military Technostructures of Policing," in *Militarizing the American Criminal Justice System: The Changing Roles of the Armed Forces and the Police*, ed. Peter B. Kraska (Boston: Northeastern University Press, 2001).

⁵⁴ Graham, *Cities Under Siege*, 198.

⁵⁵ Julie Watson, "Cops Show Marines How to Take On the Taliban," <http://www.nbclosangeles.com/news/local-beat/Cops-Show-Marines-How-to-Take-on-the-Taliban--98202989.html>, July 12, 2010.

two days. The marines then tried him, found him guilty of working with the Taliban, and released him under an agreement with local elders.

As Captain Cuomo told Khan: “This letter right here is a sworn pledge from all of your elders that they’re vouching for you and that you will never support the Taliban or fight for the Taliban ever again.” Khan then swore allegiance to the new Afghan government, and was released as a free man -- or not quite.

In exchange for his freedom, and a job cleaning a nearby canal, Khan will be supervised by a group of local elders, who in turn report to the American military. And he will himself become an informer, meeting regularly with the marines and answering their questions about his neighbors and friends.⁵⁶

Gang Wars: From Afghanistan to California

These military lessons, adapted from domestic policing and battle-tested overseas, are now being cycled back into the homeland.

Since February 2009, combat vets from Iraq and Afghanistan have been serving as advisors to police in Salinas, California, with the stated aim of applying counterinsurgency tools to local anti-gang efforts. Arranged through the Naval Postgraduate School (NPS) in nearby Monterey, the program is (officially speaking) voluntary, extra-curricular, and purely advisory -- thus avoiding the sense that the military is taking over local law enforcement. Along with their expertise, the military advisors also arrive with software, including a computer program that maps the connections between gang activity, individual suspects, and their social circles, family ties, and neighborhood connections.⁵⁷

As Salinas Chief of Police Louis Fetherolf proudly notes:

"Faculty at NPS are experts in examining violent groups around the world, including terrorists, insurgents and revolutionaries. By examining these violent groups they have developed a counterinsurgency model, which relies largely on social network analysis to determine how best to disrupt

⁵⁶ Elisabeth Bumiller, "U.S. Tries to Reintegrate Taliban Soldiers," *New York Times*, May 23, 2010.

⁵⁷ Karl Vick, "Iraq's Lessons, On the Home Front," *Washington Post*, November 15, 2009.

their violent actions and, more importantly, address the reasons for their violent behavior in the first place. NPS and SPD are working together to determine the applicability of the counterinsurgency model to violent domestic groups such as our street gangs."⁵⁸

In Salinas, the police-military partnership is occurring simultaneously with a renewal and expansion of the SPD's community policing philosophy.⁵⁹ The new community focus (encouraged, in fact, by the Naval advisors) includes increased Spanish language training, a "Gifts for Guns" trade-in event,⁶⁰ an anonymous tip hotline,⁶¹ senior-citizen volunteer programs, a larger role for the Police Community Advisory Council, and programs that provide "more youth in the community alternatives to gang lifestyles and in the process develop a growing pool of home-grown, future police officers."⁶²

Also of note are new collaborations between Salinas Police and other local, state, and federal law enforcement agencies, including the Marshals, the ATF (Alcohol, Tobacco, and Firearms), the FBI, and Immigration and Customs Enforcement.⁶³ The most spectacular product of these partnerships, so far, was a set of coordinated raids on April 22, 2010, codenamed "Operation Knockout." Chief Fetherolf recounted:

"[L]aw enforcement officials from around the state and the country assisted the Salinas Police Department and California's Department of Justice on an unprecedented offensive targeting local gang members and their associates. . . . *[O]fficers arrested over 100 gangsters and associates suspected of trafficking in narcotics and weapons. Most arrested were considered 'shot callers' or leaders of local street and prison gangs.*"⁶⁴

The operation came after months of investigation, involving Salinas Police, the Monterey

⁵⁸ Louis Fetherolf, *180-day Report to the Community* (Salinas Police Department, October 20, 2009) 9.

⁵⁹ Louis Fetherolf, *90-day Report to the Community* (Salinas Police Department, July 21, 2009) 15-16.

⁶⁰ Fetherolf, *180-day Report to the Community*, 12.

⁶¹ Fetherolf, *180-day Report to the Community*, 21.

⁶² Fetherolf, *180-day Report to the Community*, 36.

⁶³ Fetherolf, *180-day Report to the Community*, 33-4.

⁶⁴ Salinas Police Department, "Operation Ceasefire & Operation Knockout," *Report to the Community* (July 2010) 4, emphasis in original.

County Drug Task Force, the ATF, and the FBI. The sweeps themselves mobilized more than 200 law enforcement agents. In addition to the arrests, the authorities seized forty pounds of cocaine, fourteen pounds of marijuana, and a dozen guns.⁶⁵

Operation Knockout was intended, not only to disrupt the targeted gangs, but to serve as a warning to others. Deputy Police Chief Kelly McMillan said: "We're going to follow quickly with call-ins of specific groups that we know are very active. . . . We are going to tell them that what happened on the 22nd could very well happen to them."⁶⁶

The SPD's agenda for the future remains ambitious, illustrating something of the emerging, multi-faceted intelligence-sharing network. It includes plans to expand the city's video surveillance and gunfire-triangulation system, to adopt Compstat, to connect to the regional law-enforcement database COPLINK,⁶⁷ and to create "a centralized information center (Fusion Center) in Salinas for the purpose of gathering and sharing information from Federal, State and local sources."⁶⁸

Leonard A. Ferrari, provost of the Naval Postgraduate School, is enthusiastic about Salinas' potential. "The \$1 trillion invested so far in Iraq and Afghanistan could pay a dividend in American streets," he told the *Washington Post*. "The idea was, not just Salinas. . . but is there a national model for this?"⁶⁹

Ceasefire, Compstat, COIN

In fact, the Salinas collaboration, "Operation Ceasefire," is already part of national model, following a strategy developed in Boston under the same name.

In 1996, Boston's Ceasefire began with a focus on illegal handguns, but soon broadened its attention to include the gangs that used them, seeking to interrupt the cycle

⁶⁵ Julia Reynolds, "Operation Knockout: Gang Raid Targets Nuestra Familia in Salinas," *The Herald* (Monterey County), April 23, 2010.

⁶⁶ Julia Reynolds, "After Operation Knockout, Salinas Police Focus On Prevention," *The Herald* (Monterey County), April 24, 2010.

⁶⁷ Fetherolf, *180-day Report to the Community*, 16-7.

⁶⁸ Fetherolf, *180-day Report to the Community*, 10.

Fusion Centers are multi-agency operations that compile, analyze, and re-distribute. The ACLU warns that the arrangement can be used to avoid legal or policy restrictions on data collection, that the program monitors the everyday behavior of large numbers of innocent people, and that it has been used to spy on anti-war activists and organizations opposed to the death penalty. German and Stanley, "What's Wrong with Fusion Centers?"; and, German and Stanley, "Fusion Center Update."

⁶⁹ Vick, "Iraq's Lessons."

of vendetta-like violence.⁷⁰ In response to ongoing gang conflict, the Boston Police Department convened a working group consisting of law enforcement officers, social workers, academics, and members of the Black clergy.⁷¹

Researchers working with police created a list of 155 murders, mapping the crimes geographically and demographically. They examined the criminal records of both the victims and (where known) the assailants. Using this information, they created a map of various gangs, their territory, and conflict points.⁷²

Prioritizing the likely trouble-spots, police officers then sat down with gang members and gave them a clear choice: If there was gang violence in their area, both the cops and the district attorney were going to hit with everything they had:

"They could disrupt street drug activity, focus police attention on low-level street crimes such as trespassing and public drinking, serve outstanding warrants, cultivate confidential informants for medium- and long-term investigations of gang activities, deliver strict probation and parole enforcement, seize drug proceeds and other assets, ensure stiffer plea bargains and sterner prosecutorial attention, request stronger bail terms (and enforce them), and even focus potentially severe Federal investigative and prosecutorial attention on, for example, gang-related drug activity."⁷³

On the other hand, if the gang members wanted to clean up their act, the police would help them do so. Because of their coalition work, the cops came with offers of job

⁷⁰ Kennedy, "Developing and Implementing Operation Ceasefire," 17-18. Anthony A. Braga and Christopher Winship, *Creating an Effective Foundation to Prevent Youth Violence: Lessons from Boston in the 1990s* (Rappaport Institute for Greater Boston Policy Brief, September 26, 2005) 2; Anthony A. Braga and David M. Kennedy, "Reducing Gang Violence in Boston" in *Responding to Gangs: Evaluation and Research*, eds. Winifred L. Reed and Scott H. Decker (Washington, D.C.: National Institute of Justice, July 2002) 272-3.

⁷¹ Braga and Kennedy, "Reducing Gang Violence in Boston," 270.

⁷² Kennedy, "Developing and Implementing Operation Ceasefire," 20-3. For a detailed review of the mapping aspects of Ceasefire, see: David M. Kennedy, *et al.*, "The (Un)Known Universe: Mapping Gangs and Gang Violence in Boston," in *Crime Mapping and Crime Prevention*, ed. David L. Weisburd and J. Thomas McEwen (New York: Criminal Justice Press, 1997).

⁷³ David Kennedy, "Pulling Levers: Getting Deterrence Right," *National Institute of Justice Journal* (July 1998), 5.

training, drug counseling, and other services.⁷⁴ In this respect, Operation Ceasefire grew directly from the Boston Police Department's pre-existing community policing programs.

⁷⁵

Over time, ceasefire developed four levels of intervention:

"Level One was a warning, through forums or other means, to a particular group or groups to stop the violence.

Level Two was near-term street enforcement[:] . . . heavy police presence, drug market disruption, warrant service, misdemeanor enforcement, and similar actions. . . .

Level Three was a large, interagency, heavily coordinated operation . . . that was readily apparent to the target group, with sanctions remaining primarily on the State side.

*Level Four . . . was for those groups that were both violent and deemed essentially unsalvageable: undercover, gangwide investigations making heavy use of Federal sanctions and designed . . . to permanently dismantle the group."*⁷⁶

The strategy worked through direct deterrence, denying the benefits of violence and raising the costs. As importantly, "Those costs were borne by the whole gang, not just

⁷⁴ Braga and Winship, *Creating an Effective Foundation to Prevent Youth Violence*, 2; Kennedy, "Developing and Implementing Operation Ceasefire," 37; Braga and Kennedy, "Reducing Gang Violence in Boston," 274.

⁷⁵ "Before the Boston Gun Project began work on what ultimately became Operation Ceasefire, it had already created the 'network of capacity' necessary to legitimize, fund, equip, and carry out complex strategies for controlling and preventing youth violence. . . . This network was well positioned to launch an effective response to youth violence because criminal justice agencies, community groups, and social service agencies coordinated and combined their efforts in ways that could magnify their separate effects. . . . [And:] The linkages with social service agencies and other non-profit entities made it easier to convince community leaders to support Operation Ceasefire." Braga and Winship, *Creating an Effective Foundation to Prevent Youth Violence*, 4-5.

⁷⁶ David M. Kennedy, *et al.*, "Developing and Implementing Operation Ceasefire," in *Reducing Gun Violence: The Boston Gun Project's Operation Ceasefire* (Washington, D.C.: U.S. Department of Justice, National Institute of Justice, September 2001) 42-3, emphasis added.

For an overview of the Ceasefire strategy, see: Kennedy, "Pulling Levers."

For an analysis of the importance of community policing in creating the conditions for Ceasefire's success, see: Braga and Christopher Winship, *Creating an Effective Foundation to Prevent Youth Violence*.

the shooter."⁷⁷ So the cops could begin applying meaningful pressure before identifying an individual suspect, and the gang had an incentive to keep their members under control and maintain the peace.

The key elements of Operation Ceasefire -- social network analysis, community policing, inter-agency cooperation, and a direct approach to deterrence -- were quickly replicated and taken further in other cities, intersecting trends like zero-tolerance policing and the Compstat program. A report from the Justice Department's Office of Community Oriented Policing Service, *Street Gangs and Interventions: Innovative Problem Solving with Network Analysis*, provides a case study illustrating the result:

In the mid-1990's Newark's police were being remolded according to the pattern set by Giuliani's New York. The director of the Newark Police Department, Joe Santiago, introduced a Compstat system and, in 1996, proposed a partnership with Rutgers University professor George Kelling -- famous as one of the authors of the "Broken Windows" theory underlying police zero-tolerance campaigns.⁷⁸ This partnership coalesced as the Greater Newark Safer Cities Initiative (GNSCI).⁷⁹

Slowly, Santiago built a working group including cops, scholars, social workers, the clergy, and even public defenders. It began by focusing on a small number of repeat offenders, using the same deterrence model developed in Ceasefire. Then, in 2003, GNSCI turned its attention to gangs, leading it to look beyond the city limits. The North Jersey Gang Task Force was born.⁸⁰ Coordinating with law enforcement agencies statewide, the Rutgers researchers began to collect

"data on such issues as gang territory, the role, nature, and extent of violence and crime, recruitment and initiation rituals, the extent of female membership, size, history, the role of families, and other topics of interest. In addition, researchers began to gather information on the

⁷⁷ Kennedy, "Pulling Levers," 6.

⁷⁸ James Q. Wilson and George L. Kelling, "Broken Windows," *Atlantic Monthly* (March 1982).

⁷⁹ Jean M. McGloin, *Street Gangs and Interventions: Innovative Problem Solving with Network Analysis* (Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services, September 23, 2005) 9.

⁸⁰ McGloin, *Street Gangs and Interventions*, 11-13.

criminal histories of all identified gang members."⁸¹

Once the data was assembled, the researchers, following Boston's example, used it to map gang territory and perform a social network analysis:

"Such an analysis provided insight into why particular geographic areas may experience violence caused by a contentious relationship among gangs or sets and the allegiances and rivalries that could influence the focus of an intervention or suppression program."

After charting the relationships between gangs, they then took the analysis to the individual level --

"defining the relationships among known gang members and their associates[:] . . . who hangs out and commits crime together ('runs together'), who has been incarcerated together, who is related to each other, who is a co-arrestee or co-defendant with whom, and other relationship dimensions. . . ."

This exercise "provid[ed] insight into the structure of the gangs as well as into the various social positions that members occupy within the gangs."⁸² By diagramming these relationships, researchers were able to distinguish between core members and those only marginally involved.

Such information was crucial for making both tactical and strategic decisions. Police could approach individual members differently, based on their role in the gang and their level of commitment. They could also identify the pressure points, the weak links, and know where to strike for maximum effect.

"Network analysis also allows one to identify people who hold structurally important positions within the gang networks. Cut points, people who are

⁸¹ McGloin, *Street Gangs and Interventions*, 14.

⁸² McGloin, *Street Gangs and Interventions*, 15- 7.

the only connection among people or groups of people, may be ideal selections for spreading a deterrence message or for affecting the structure and organization of the street gangs."⁸³

Unlike Boston, where the focus was strictly on stopping gang *violence*,⁸⁴ in New Jersey the aim was to disrupt the gangs themselves.

The Black Snake

Under Ceasefire, in Salinas as in Boston, gang members are taken to police headquarters for all-day meetings. They're given a stern warning to quit the gang life, and offered services like job counseling and tattoo removal.⁸⁵ And at the same time, those associated with gang activity face persistent harassment.

As in New Jersey, Salinas' gang suppression campaign is a regional coalition effort. The main group responsible for such work is the Monterey County Gang Task Force, called "The Black Snake" by youths in the community. The task force has 17 members, drawn from local police and sheriffs departments, the California Highway Patrol, and the state Department of Corrections. Wearing distinctive black uniforms and driving black cars, Task Force members conduct mass-arrest "round-ups,"⁸⁶ make random traffic stops, and regularly search the homes of gang members on parole or probation.⁸⁷ The sheer volume of such activity is astonishing: Since it was formed in 2005, the Task Force has been responsible for 21,000 vehicle or pedestrian stops, 5,000 parole and probation "compliance" searches, and 2,800 arrests.⁸⁸

⁸³ McGloin, *Street Gangs and Interventions*, 18. See also: Phil Williams, "Transnational Criminal Networks," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica: Rand, 2001) 91-95.

⁸⁴ Kennedy, "Pulling Levers," 4.

⁸⁵ Scott Kraft, "Aggressive Crackdown Targets Long-Entrenched Salina Gangs." *Los Angeles Times*. June 16, 2010.

⁸⁶ Salinas Police Department, "Operation Ceasefire & Operation Knockout," 4.

⁸⁷ Scott Kraft, "Aggressive Crackdown Targets Long-Entrenched Salina Gangs." *Los Angeles Times*. June 16, 2010.

⁸⁸ Joseph E. Long, *A Social Movement Theory Typology of Gang Violence* (Monterey, California: Naval Postgraduate School, June 2010) 37.

Regardless, the rate of violent crime has not appreciably decreased. Long, *Social Movement Theory Typology*, 35.

In this context, as California's Gang and Youth Violence Policy Director Paul Seave explains, Operation Knockout "fits perfectly into the Ceasefire strategy. . . . Ceasefire depends on following through on commitments that if the violence doesn't stop, force will be applied vigorously."⁸⁹

Carrots and Sticks, Hearts and Minds

Operation Ceasefire and its progeny work chiefly through the "Cost/Benefit" (or "Coercion") approach to counterinsurgency. The government provides an admixture of incentives and deterrents to shape the choices of potential rebels. As Rand describes the approach:

"Populations were viewed as rational actors that would respond in more or less predictable ways to incentives and sanctions from . . . insurgent and counterinsurgent. Ultimately, what mattered to both [sides] was not the population's attitudes but its actions."⁹⁰

At the same time, in developing Ceasefire, the police made sure to align other sources of legitimacy -- social services, community organizations, the clergy -- with its efforts, thus simultaneously increasing its leverage and heading off potential resistance. For example, in Boston, the Ceasefire coalition included Black ministers who had been vocal critics of the police. These men of the cloth began advising the cops in their anti-gang work, and eventually "sheltered the police from broad public criticism."⁹¹

The other major approach to COIN -- the older and more famous "hearts and minds" strategy -- operates by a somewhat different logic, focusing on "the problems of modernization and the insurgent need for popular support." As Rand explains:

"The answer was to restore the hope of the people and gain their support for the

⁸⁹ Quoted in Julia Reynolds, "Operation Knockout."

⁹⁰ Gompert and Gordon, *On Other War*, 25.

⁹¹ Braga and Winship, *Creating an Effective Foundation to Prevent Youth Violence*, 6. See also: Kennedy, "Developing and Implementing Operation Ceasefire," 9-10; Braga and Kennedy, "Reducing Gang Violence in Boston," 281-3.

government. In order to do this, COIN would consist of providing the people security from predations by government and insurgent forces and reducing the negative consequences of development while enhancing the positive aspects. Increasing political rights of the people, improving standards of living, and reducing corruption and abuse of government power were key prescriptions. . . ."⁹²

We can see the "Hearts and Minds" approach employed in a separate domestic experiment -- the federally funded "Weed and Seed" program.

Weed and Seed: Clear-Hold-Build

Weed and Seed was conceived in 1991. It gained prominence a year later as part of the federal response to widespread rioting after the acquittal of four Los Angeles cops who had been videotaped beating Black motorist Rodney King. Since that time, it has been implemented in over 300 neighborhoods nationwide.⁹³

The Department of Justice describes the project like this:

"The Weed and Seed strategy is based on a twopronged approach:

1. Law enforcement agencies and criminal justice officials cooperate with local residents to 'weed out' criminal activity in the designated area.
2. Social service providers and economic revitalization efforts are introduced to 'seed' the area, ensuring long-term positive change and a higher quality of life for residents."⁹⁴

In terms of strategy, Weed and Seed closely resembles the military process called "Clear-Hold-Build." As FM 3-24 elaborates: "Create a secure physical and psychological environment. Establish firm government control of the populace and area. Gain the

⁹² Gompert and Gordon, *On Other War*, 25

⁹³ *Weed and Seed Implementation Manual*, 1.

⁹⁴ *Weed and Seed Implementation Manual* 1.

populace's support."⁹⁵

Clearing and *holding* refer to the removal and exclusion of hostile elements -- whether insurgents or gangs. *Building*, on the other hand, means both, literally, repairing infrastructure and, more metaphorically, gaining trust and winning support.⁹⁶ However, even *building* includes an element of force:

"Progress in building support for the HN [Host Nation] government requires protecting the local populace. . . . To protect the populace, HN security forces continuously conduct patrols and use measured force against insurgent targets of opportunity. . . . Actions to eliminate the remaining covert insurgent political infrastructure must be continued. . . ."⁹⁷

The domestic analogy is pretty straightforward. As one police chief described the role of paramilitary units in his community policing strategy:

"[The] only people that are going to be able to deal with these problems are highly trained tactical teams with proper equipment to go into a neighborhood and clear the neighborhood and hold it; allowing community policing officers to come in and start turning the neighborhood around."⁹⁸

In such campaigns, the relationship between community policing and militarization is

⁹⁵ (FM 3-24, 5-50 and 5-51). Beers points to Weed and Seed as a strategy for progress in Afghanistan. Beers, *Community-Oriented Policing and Counterinsurgency*, 70.

⁹⁶ The *Counterinsurgency* Field Manual, lists "Sample tasks" such as "Collecting and clearing trash from the streets"; "Removing or painting over insurgent symbols or colors"; "Building and improving roads;" "Securing, moving, and distributing supplies;" and "Building and improving schools and similar facilities." FM 3-24, 5-70.

⁹⁷ FM 3-24, 5-68.

⁹⁸ Peter B. Kraska and Victor E. Kappeler, "Militarizing American Police: The Rise and Normalization of Paramilitary Units," in *The Police and Society: Touchstone Readings*, ed. Victor E. Kappeler (Prospect Heights: Waveland Press, 1999), 473.

See also: Matthew T. DeMichele and Peter B. Kraska, "Community Policing in Battle Garb: A Paradox or Coherent Strategy," in *Militarizing the American Criminal Justice System: The Changing Roles of the Armed Forces and the Police*, ed. Peter B. Kraska (Boston: Northeastern University Press, 2001) 96.

especially clear. They're not competing or contradictory approaches. They work together, simultaneously or in series. One does the weeding; the other, the seeding.⁹⁹

The implications are not lost on those subject to this sort of campaign. "They're gunning for us," Omari Salisbury, a Seattle teenager, said when he heard about Weed and Seed. "They're gunning for Black youth."¹⁰⁰

The Politics of Gang Suppression

As we can see, police anti-gang campaigns typically combine a variety of elements analogous to those in counterinsurgency: the creation of databases listing suspected gang members; the mapping of the social environment in which the gang operates, illustrating connections between gang members, their associates, family ties, *etc.*; the development of community contacts, especially with members of the clergy, school officials, social service workers, and so on. These intelligence efforts are then paired with a campaign of persistent low-level harassment -- stops, searches, petty citations, and the like. Each instance of harassment offers police the opportunity to collect additional information on the gang network while at the same time creating an inhospitable environment for those associated with gang activity. At a broader level, the police will also engage in efforts disruptive of ordinary social life in gang-affected areas, such as cordoning, saturating, or sweeping select locations (*e.g.*, parks, streets, or bars) or targeted events (ballgames, parties, car shows).¹⁰¹

⁹⁹ The Justice Department's *Implementation Manual*'s "Exhibit 8-1. Local Drug Enforcement Tactics" lists several practices indicative of a level of militarization, including: saturation patrols, "crackhouse raids," and roadblocks and checkpoints. *Weed and Seed Implementation Manual* 62.

The Manual's chapter on "Community Policing," meanwhile, advises, "Develop an Information and Communication Network: . . . The information network includes intelligence (*e.g.*, tips from residents or informants) and routinely collected records (*e.g.*, calls for service, crime reports, field interrogation information). Several police agencies have automated information networks that provide local officers with data useful for problem solving and community engagement." *Weed and Seed Implementation Manual* 67-8.

¹⁰⁰ Quoted in Dick Lilly, "City Urged to Bury Weed and Seed Plan," *Seattle Times*, March 27, 1992.

When Seattle applied for Weed and Seed funds in 1992, the program faced opposition from dozens of groups, including the ACLU, the Fellowship of Reconciliation, the Church Council of Greater Seattle, and the King County Labor Council. A community clinic even refused a \$30,000 grant, rather than be associated with the program. Dick Lilly, "Weed and Seed Not Likely This Year," *Seattle Times*, September 15, 1992; and Kate Shatzkin, "'Weed, Seed' Aid for Clinic Rejected," *Seattle Times*, June 11, 1992.

¹⁰¹ For a discussion of gang suppression activities and their impact on communities of color, see: Felix M.

In the most advanced campaigns, police sometimes take the further step of strategically *causing* gang conflict. Following the 1992 Los Angeles riots, for example, police did what they could to wreck a city-wide truce between the Bloods and the Crips. The cops didn't just attack negotiating meetings and inter-gang social events, but also engaged in some underhanded tactics to create friction: covering one gang's graffiti with another's, or arresting a Blood only to release him deep in Crip territory. This occurred, not only in a context of widespread anger and recent unrest, but also at a point in which the gangs themselves were becoming increasingly politicized.¹⁰²

Indeed, sometimes anti-gang campaigns take an obviously political form. In Portland, Oregon, where I live, the Portland Police Bureau's Gang Enforcement Team managed a city-wide anti-skinhead campaign in the late 1980s and early 90s (giving special attention, it should be noted, to *anti-racist* skinheads).¹⁰³ The "gang" label, here, did ideological work, branding both Nazi and anti-Nazi activity as criminal, and thus implicitly de-politicizing the conflict and the state's role in it. A decade later, the GET was used to target the anarchist punk scene following the 1999 WTO protests in nearby Seattle.¹⁰⁴

Padilla, *Gangs as an American Enterprise* (New Brunswick, New Jersey: Rutgers University Press, 1992), 85; and Randall G. Sheldon *et al.*, *Youth Gangs in American Society* (Belmont, California: Wadsworth, 2001), 244.

¹⁰² Mike Davis, "Understanding L.A.: The New Urban Order [interview with *CovertAction Information Bulletin*]," in *USA: A Look at Reality*, (Hyattsville, Maryland: Equal Justice USA/Quixote Center: July 1992), 2; Malcolm W. Klein, *The American Street Gang: Its Nature, Prevalence, and Control* (New York: Oxford University Press, 1995), 165; and Irving A. Spergel, *The Youth Gang Problem: A Community Approach* (New York: Oxford University Press, 1995) 191.

Accompanying the Davis interview is a photograph by Michael Zinzun showing uniformed cops "tagging" over gang graffiti. Davis 2.

¹⁰³ Coalition for Human Dignity, *Report of the Community Defense Project on Organized Neo-Fascists in Portland, Oregon* (May 18, 1990).

For the police perspective, see Loren Christensen, *Skinhead Street Gangs* (Boulder, Colorado: Paladin Press, 1994), especially pages 56-63.

More recently, in 2010, after a local anti-racist was shot, reportedly by members of the Nazi group Volksfront, an unnamed Portland cop told reporters that the conflict was not over politics, but gang turf. "I'm not sure how either [group] can claim to be better than the other," he said. Quoted in Marcus Griffith, "Racists and Anti-Racists," *Vancouver Voice*, August 4, 2010. See also: Marcus Griffith, "Vancouver's Volksfront," *Vancouver Voice*, May 10, 2010.

¹⁰⁴ Kristian Williams, "The Criminalization of Anarchism, Part Two: Guilt by Association, Questionable Confessions, and Mandatory Minimums" in *Confrontations: Selected Journalism* (Portland, Oregon: Tarantula, 2007).

It is worth noting, in this context, that the L.A. County Sheriffs Office's John Sullivan named the anti-WTO black bloc, criminal gangs, and football hooligans, as "The Vanguard of Net-War in the Streets." John P. Sullivan, "Gangs, Hooligans, and Anarchists: The Vanguard of Netwar in the Streets," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa

But even in their routine form, anti-gang efforts are always implicitly political, especially as they become permanent features of life in poor Black and Latino communities. Though ostensibly aimed at preventing gang violence, counter-gang campaigns inevitably lead police to monitor the community as a whole.¹⁰⁵ Disproportionate attention, especially when paired with lower -- or "zero" -- tolerance for disorder, then contributes to higher rates of arrest and incarceration.

Mike Davis described the government's response to the 1992 Los Angeles riots in military terms:

“In Los Angeles I think we are beginning to see a repressive context that is literally comparable to Belfast or the West Bank, where policing has been transformed into full-scale counterinsurgency (or ‘low-intensity warfare,’ as the military likes to call it) against an entire social stratum or ethnic group.”¹⁰⁶

The Suppression of Gang Politics

The insurgent/gang analogy is not as outlandish as it might first seem.¹⁰⁷ In practice, gangs don't just engage in criminality and violence, they also *regulate* criminality and violence -- and, by extension, help to structure their communities and control street life. In this respect, gangs can be seen acting in ways that are essentially state-like.

Further, as John Sullivan, an L.A. County Sheriffs Deputy, writes in one Rand report:

Monica: Rand, 2001) 120-3.

¹⁰⁵ A Fresno cop explains the intended scope of his department's gang files: “If you're twenty-one, male, living in one of these neighborhoods, been in Fresno for ten years and you're *not* in our computer—then there's definitely a problem.” Parenti, *Lockdown America*, 111, emphasis added.

¹⁰⁶ Davis, "Understanding L.A.," 2. For similar assessments, see: Graham, *Cities Under Siege*, 218; and Ana Arana, "How Street Gangs Took Central America," *Foreign Affairs* (May-June 2005) 100.

¹⁰⁷ For analytic comparisons between gangs and insurgencies, from a military standpoint, see: Long, *Social Movement Theory Typology*; Max G. Manwaring, *Street Gangs: The New Urban Insurgency* (Carlisle, Pennsylvania: Strategic Studies Institute: March 2005); and, John P. Sullivan, "Future Conflict: Criminal Insurgencies, Gangs and Intelligence" *Small Wars Journal*, <http://smallwarsjournal.com/blog/journal/docs-temp/248-sullivan.pdf>. May 31, 2009.

"[S]ome [gangs] have begun to adopt varying degrees of political activity. At the low end, this activity may include dominating neighborhood life and creating virtual 'lawless zones,' application of street taxes, or taxes on other criminal actors. Gangs with more sophisticated political attributes typically co-opt police and government officials to limit interference with their activities. At the high end, some gangs have active political agendas, using the political process to further their ends and destabilize governments."¹⁰⁸

Among the examples Sullivan cites are the Gangster Disciples, a gang with 30,000 members in 35 states. In addition to employing themselves in the drug trade, "GD members infiltrate police and private security agencies, sponsor political candidates, register voters, and sponsor protest marches."¹⁰⁹ Other gangs have been active in resistance against gentrification, loan sharks, slum lords, price gouging, and police brutality.¹¹⁰

Historically, the Black Panther Party recognized the political potential of gangs and their members. Most strikingly, the Los Angeles chapter was formed by a former gang leader, Alprentice "Bunchy" Carter of the Slauson Renegades.¹¹¹ In Philadelphia, in the late 60s, the Panthers organized a series of gang conferences and tried to use negotiations to quell gang violence. (Their success was limited, but observable: The Panthers couldn't stop the gangs from fighting altogether, but when the BPP dissolved, gang violence noticeably increased.) The Panthers also directed some of their public education and recruitment efforts toward gang members, and urged gangs to earn respect by serving the community. Some gangsters did, in fact, enlist to help in the Panthers' free breakfast program, and a few went on to become full Party members.¹¹²

One cannot understand gangs only as a criminal phenomena. They exert power;

¹⁰⁸ Sullivan, "Gangs, Hooligans, and Anarchists," 102.

¹⁰⁹ Sullivan, "Gangs, Hooligans, and Anarchists," 113-4.

¹¹⁰ Martín Sánchez Jankowski, *Islands in the Street: Gangs and American Urban Society* (Berkeley: University of California Press, 1991), 11-12 and 179-192.

¹¹¹ Judson L. Jeffries and Malcolm Foley, "To Live and Die in L.A.," in *Comrades: A Local History of the Black Panther Party*, ed. Judson L. Jeffries (Bloomington: Indiana University Press, 2007) 261.

¹¹² Omari L. Dyson, *et al.*, "'Brotherly Love Can Kill You': The Philadelphia Branch of the Black Panther Party," in *Comrades: A Local History of the Black Panther Party*, ed. Judson L. Jeffries (Bloomington: Indiana University Press, 2007) 228-30.

they operate politically. Therefore, the state's anti-gang efforts have to be understood politically as well. The police are not only (or even mainly) fighting crime, enforcing the law, or preventing violence -- they are also disrupting and dis-organizing an incipient political force, striking against it before it can become a real nexus of resistance.

In fact, by applying the techniques and analysis of counterinsurgency to counter-gang campaigns, the government tacitly admits that there is a political dimension to what is ordinarily presented as pure criminality. Insurgency and counterinsurgency are, together, a struggle over legitimacy. By applying the COIN framework domestically, the government concedes that its legitimacy is being challenged and that the challengers (however localized and weak) are rivals, or potential rivals, with independent claims to legitimacy and distinct spheres of influence.

COINing the Green Scare

It is not hard to see how COIN strategies and techniques could be applied, not only against gangs or jihadists, but against the left as well. Military strategists are certainly considering the idea.

John Allison, an anthropologist briefly enrolled in the Army's "Human Terrain System" program, reported war game exercises involving military action in "Lakeland," an imaginary secessionist state to the northeast of Kansas City. In, this training scenario Human Terrain Teams are sent in to Lakeland in response to unrest -- specifically, anti-coal actions by the Sierra Club and more radical groups, including the Earth Liberation Front. The Human Terrain Team students were assigned the following tasks:

- "1. 'Find out more details on the criminal activity.'
2. Find out the best conduits to pass 'information' (PsyOps and InfoOps) to the local population. . . .
- [3. P]roduce a 'Research Plan' to understand the situation at the IATAN power plant -- people's concerns, desires, etc., and identify those who were 'problem-solvers' and those who were 'problem-

causers,' and the rest of the population whom would be the target of the information operations to move their Center of Gravity toward that set of viewpoints and values which was the 'desired end-state' of the military's strategy."¹¹³

Again, military theory seems to be following police practice. For the past decade, law enforcement agencies have engaged in a concentrated campaign broadly targeting the environmental and animal rights movements. The centerpiece of the campaign was "Operation Backfire," a set of coordinated arrests launched in December 2005. The Backfire defendants were accused of a series of Earth Liberation Front and Animal Liberation Front arsons from the late 1990s -- activities the FBI characterized as "domestic terrorism."¹¹⁴ A few of those arrested fought the charges, or plead guilty without implicating others; most, however, gave evidence against their comrades in hopes of leniency at sentencing.

The months that followed showed a sharp escalation in repression of the environmental movement, in what came to be called the "Green Scare." By the end of 2006, in addition to the Backfire arrests, six members of Stop Huntington Animal Cruelty were convicted on terrorism charges (essentially for running an animal-rights website), and three young people were arrested in connection to an ELF-style conspiracy fabricated by a paid provocateur. The following year another activist began wearing a wire to collect evidence against his partners in an earlier ELF arson.¹¹⁵

Much of this activity was centered in Eugene, Oregon, and it followed a pattern established there during the period since 1999. The anarchist journal *Rolling Thunder* describes the cops' approach:

¹¹³ Quoted in David Price, "Human Terrain Systems Dissenter Resigns, Tells Inside Story of Training's Heart of Darkness," *CounterPunch*, February 15, 2010. Paragraph breaks added for clarity.

Allison resigned before the exercise was finished.

¹¹⁴ Department of Justice, "Eleven Defendants Indicted on Domestic Terrorism Charges [press release]," January 20, 2006, http://www.justice.gov/opa/pr/2006/January/06_crm_030.html; and, Will Potter, "The Green Scare," *Vermont Law Review* (2009) 673.

¹¹⁵ Will Potter, "What is the Green Scare?" *Green is the New Red*, September 1, 2008, <http://www.greenisthenewred.com/blog/green-scare/>; Will Potter, "Feds Hope to Set an Example with 'Eco-Terrorist Who Refused to Snitch,'" *Green is the New Red*, February 3, 2009, <http://www.greenisthenewred.com/blog/marie-mason-refusal-to-snitch/993>; and, "Green Scare: The Timeline," *Earth First! Roadshow* (2009), <http://earthfirstroadshow.files.wordpress.com/2009/05/gs-timeline-for-website.pdf>.

"What we know of the early Backfire investigation points to a strategy of generalized monitoring and infiltration. While investigators used increasingly focused tools and strategies as the investigation gained steam—for example, sending 'co-operating witnesses' wearing body wires to talk to specific targets—they started out by sifting through a whole demographic of counter-cultural types. . . . Police accumulated tremendous amounts of background information even while failing to penetrate the circles in which direct action was organized. The approximately 30,000 pages of discovery in the Oregon cases contain a vast amount of gossip and background information on quite a few from the Eugene community."¹¹⁶

Writing in the *Vermont Law Review*, Will Potter, who probably knows more about the Green Scare than anyone outside of law enforcement, argues that the target of Backfire and similar operations was not necessarily the ELF *per se*, but the broader environmental and animal rights movement:

"The mainstreaming of these movements, and the shifts in public opinion that they bring, have potentially grave implications for the corporations and industries that benefit from the abuse of animals and the destruction of the environment. These coordinated attacks on the animal-rights and environmental movements are not simply meant to deter illegal activity, they are meant to destroy movements that pose an ideological threat. . . . The point is to protect corporate profits by instilling fear in the mainstream animal-rights and environmental movements—and every other social movement paying attention—and make people think twice about using their First Amendment rights. It's not the illegal activists that are the targets; it's the legal, above-ground activists."

¹¹⁶ "Green Scared? Preliminary Lessons of the Green Scare," *Rolling Thunder* (Spring 2008) 30.

Potter also offered this warning, "if these attacks are not confronted, corporations and the government will simply move on to other social movements."¹¹⁷

Part Three: Preserving Order, Preventing Change

Hard and Soft

I began this paper by outlining, in some detail, the basic principles of counterinsurgency theory, the intelligence needs that accompany it, and its direct application in both (foreign) military and (domestic) policing contexts. I've explained something of the methodology of Social Network Analysis, and the process by which its insights into both insurgent organizations and the surrounding population are translated into direct coercion and bids to win popular support. I have suggested, more or less explicitly, that if the left wants to understand the repression it faces, it should study the way the U.S. responds to forces as varied as the Taliban, the Gangster Disciples, and the ELF. And I have stated, and repeated (perhaps tiresomely), that it is the *political* dimension of insurgency and counterinsurgency that really counts. I have, in other words, stressed the *revolutionary* aspect of revolutionary warfare, rather than the *warfare* aspect.

And yet, thus far, I have focused chiefly on the "hard" side of repression -- the direct coercion, the forceful disruptions, the criminalization and incarceration, the violence. Now we need to look at the "soft" side -- the strategic use of concessions, the promise of representation and access, the co-optation of leadership, and, comprising all of these, the *institutionalization* of dissent.¹¹⁸ These elements represent, at this point, the

¹¹⁷ Potter, "Green Scare," 685-6.

¹¹⁸ "Institutionalization . . . is composed of three main components: First, the *routinization* of collective action, such that challengers and authorities can both adhere to a common script, recognizing familiar patterns as well as potentially dangerous deviations. Second, *inclusion* and *marginalization*, whereby challengers who are willing to adhere to established routines will be granted access to political exchanges in mainstream institutions, while those who refuse to accept them can be shut out of conversations through either repression or neglect. Third, *cooptation*, which means that challenges alter their claims and tactics to ones that can be pursued without disrupting the normal practice of politics." David S. Meyer and Sidney Tarrow, "A Movement Society: Contentious Politics for a New Century," in *The Social Movement Society: Contentious Politics for a New Century*, ed. David S. Meyer and Sidney Tarrow, (Lanham, Maryland: Rowman and Littlefield, 1998) 21.

state's most typical response to opposition from the left. And, by these means, the state does not only achieve control and exercise power *over* the organizations of the left, but *through* them.

Stages and Strategies

In its earlier stages, repression may be hard to recognize for exactly the same reasons that a proto-insurgency is -- because everything seems normal. We should remember, however, that the authorities aren't just *preparing* for unrest, they're actively *preempting* opposition. They do that by broadly monitoring the community, building alliances, channeling community efforts into projects they can control, and disrupting networks and social ties that might otherwise form the basis for resistance.

Of course, as COIN moves into its later stages it will become increasingly military in character. Both the overt use of force and covert surveillance, infiltration, and disruption will increase. Emergency powers may be granted, civil liberties suspended, and the life of the overall population increasingly restricted.¹¹⁹

But as the crisis progresses to higher levels, the work of lower stages continues. Smart revolutionaries don't *stop* organizing as they escalate their tactics; they use their actions to help build their organizations. Likewise, the security forces don't stop their efforts at intelligence gathering or alliance building, but use those efforts in support of their more bellicose activities.

Of course, the aim of any counterinsurgency campaign is a return to normal -- that is, not peace, exactly, but the lowest level of manageable conflict. In effect, this is a return to the proto-insurgency stage: Opposition is either channeled into safe, institutional forms, or suppressed through normal police and intelligence activity.¹²⁰

¹¹⁹ The Special Forces Manual on Foreign Internal Defense, for example, lists some possibilities: "curfews or blackouts, travel restrictions, and restricted residential areas such as protected villages or resettlement areas[;] Registration and pass systems and control of . . . critical supplies such as weapons, food, and fuel. . . [;] Checkpoints, searches, roadblocks; surveillance, censorship, and press control; and restriction of activity that applies to selected groups (labor unions, political groups and the like). . . ." FM 31-20-3, 3-23

¹²⁰ Celeski, *Policing and Law Enforcement in COIN*, 29.

The French military strategist David Galula, a contemporary of Kitson's, notes that even when the fighting is over, the repression is not: "The policeman starts gathering intelligence right from the beginning; his role does not end when the political cells have been destroyed, because the insurgent will keep trying to build new ones." Galula, *Counter-Insurgency Warfare*, 88.

Kitson summarizes the overall process:

"In practical terms the most promising line of approach lies in separating the mass of those engaged in the [revolutionary] campaign from the leadership by the judicious promise of concessions, at the same time imposing a period of calm by the use of government forces. . . . Although with an eye to world opinion and to the need to retain the allegiance of the people, no more force than is necessary for containing the situation should be used, conditions can be made reasonably uncomfortable for the population as a whole, in order to provide an incentive for a return to normal life and to act as a deterrent towards a resumption of the campaign.

Having once succeeded in providing a breathing space by these means, it is most important to do three further things quickly. The first is to implement the promised concessions. . . . The second is to discover and neutralize the genuine subversive element. The third is to associate as many prominent members of the population, especially those who have been engaged in non-violent action, with the government. This last technique is known in America as co-optation. . . ." ¹²¹

Broadly speaking, counterinsurgency offers two approaches in dealing with resistance, and they must be used selectively. Some adversaries, especially moderate elements -- perhaps the majority involved in the movement -- may be co-opted, bought off, and appeased. Others, the more recalcitrant portion, must be forcefully disorganized, disrupted, deterred, or destroyed. The balance of concessions and coercion will be apportioned accordingly. Some adversaries win new posts -- offices in a "reformed" administration, or jobs in "responsible" nonprofits, labor unions, or progressive think tanks. They gain access, inclusion, or representation in exchange for

¹²¹ Kitson, *Low Intensity Operations*, 87.

Byman argues similarly: "The ideal allies for a government implementing control are, in fact, nonviolent members of the community the would-be insurgents seek to mobilize. . . . If regimes can infiltrate -- or, better yet, cooperate with -- mainstream groups they are often able to gain information on radical activities and turn potential militants away from violence." Daniel Byman, *Understanding Proto-Insurgencies* (Santa Monica: Rand, 2007) 24.

working within the existing institutional framework. The others will face harsher outcomes -- including, for example: imprisonment, exile, and direct violence. Whatever the approach in a particular case, the important thing is that the opposition is neutralized -- rendered harmless, made controllable, and exploited as either the object or the tool of state power.

This strategy, too, is equally evident at home and abroad.

The Military-NGO Complex

It is hardly surprising that the state would use its resources -- including its money -- to advance its own agenda. Foreign aid has thus often been criticized as an instrument of imperialism, even when it is distributed indirectly through nongovernmental or humanitarian organizations (NGOs or NGHOs).¹²²

Still, in October 2001, as the U.S. began its war against Afghanistan, Colin Powell managed to embarrass NGO leaders with his praise for their work. Speaking at the National Foreign Policy Conference for Leaders of Nongovernmental Organizations, Powell -- the former General, the founding Chairman of the nonprofit America's Promise Alliance, and, at the time, the Secretary of State -- told the assembled humanitarians: "[J]ust as surely as our diplomats and military, American NGOs are out there serving and sacrificing on the front lines of freedom. . . . [NGOs] are such a force multiplier for us, such an important part of our combat team."¹²³

Later, guidelines negotiated by representatives of the military and the major humanitarian groups discouraged any repetition of Powell's gaffe, specifying that "U.S. Armed Forces should not describe NGHOs as 'force multipliers' or 'partners' of the military, or in any other fashion that could compromise their independence and their goal to be perceived by the population as independent."¹²⁴

¹²² See, for examples: Arundhati Roy, "Public Power in the Age of Empire," *Democracy Now*, August 23, 2004, http://www.democracynow.org/2004/8/23/public_power_in_the_age_of#; Ji Giles Ungpakorn, "NGOs: Enemies or Allies," *International Socialism* (October 2004); Yves Engler, "Occupation by NGO," *CounterPunch*, August 13-15, 2010; James Petras, "NGOs: In the Service of Imperialism," *Journal of Contemporary Asia*, 29.4 (1999).

¹²³ Colin Powell, "Remarks to the National Foreign Policy Conference for Leaders of Nongovernmental Organizations," October 26, 2001, http://avalon.law.yale.edu/sept11/powell_brief31.asp

¹²⁴ United States Institute of Peace, *Guidelines for Relations between U.S. Armed Forces and Non-*

But the truth remained. The Rand study *Networks and Netwars* outlined "a range of possibilities" for the military's use of international non-profits,

"from encouraging the early involvement of appropriate NGO networks in helping to detect and head off a looming crisis, to working closely with them in the aftermath of conflicts to improve the effectiveness of U.S. forces still deployed, to reduce the residual hazards they face, and to strengthen the often fragile peace."¹²⁵

One result of this perspective is that the aid money, and thus NGO attention, increasingly follows the state's priorities -- and its military's priorities in particular. For instance, in 2010 alone the U.S. awarded \$114 million to aid groups working in Yemen, with the explicit goal of "improving the livelihood of citizens in targeted communities and improving governance capabilities."¹²⁶

"[D]evelopment priorities follow the battle space," David Rieff writes in *The New Republic*. "[D]evelopment is a continuation of war by other means."¹²⁷

How Nonprofits Protect the State

The military and spy agencies have long understood the various uses to which they can put Non-Governmental Organizations overseas -- funding covert ops, collecting intelligence, delivering aid, and variously stabilizing or destabilizing the area of operations, legitimizing or subverting the government, according to the United States' interests and agenda.

The partnerships advocated by community policing strategists use non-profits, and even some grassroots community organizations, in much the same way. Through these partnerships, police gain access to the communities they are tasked with controlling. The

Governmental Humanitarian Organizations in Hostile or Potentially Hostile Environments (no date).

¹²⁵ John Arquilla and David Ronfeldt, "Summary," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica: Rand, 2001) x.

¹²⁶ Quoted in David Rieff, "How NGOs Became Pawns in the War on Terrorism," *The New Republic*, August 3, 2010.

¹²⁷ Rieff, "How NGOs Became Pawns."

cops bring their resources -- funding, leverage with other parts of the state, and coercive muscle -- along with a promise to listen. Their partners help identify community problems and mobilize community resources; in other words, they provide the cops with information and help facilitate community cooperation with policing. In the process, a friendly face is put on police action, and a bit more money and legitimacy is made available to the non-profits to aid in their mission.

Of course, the police pursue these partnerships, and provide the resources, selectively, according to their own agenda. Thus the state uses its influence to suppress radical groups and support moderate ones. And these same partnerships, which are defined and controlled by the police, serve to discipline the community organizations, since "unacceptable" actions will undoubtedly cost them.

Police can thus team up with progressive non-profits to channel and control political opposition, moving it in safe, institutional, and reformist directions, rather than in more radical or militant directions.

The Marshal Plan

For example, consider the efforts of liberal non-profits to contain community anger after transit police shot and killed an unarmed Black man in Oakland, California.

Oscar Grant was killed on January 1, 2009. A week later, on January 7, a protest against the police turned into a small riot.¹²⁸ Organizers with the Coalition Against Police Executions (CAPE) -- a group largely composed of local progressive non-profits and Black churches -- denounced the violence. One CAPE leader said that he wept watching the riots on television, feeling that years of hard work were being "destroyed by anarchists."¹²⁹

But -- likely because of the unrest -- the cop in the case, Johannes Mehserle, was arrested and charged with murder.¹³⁰ Before the riots there had been no statement from

¹²⁸ George Ciccariello-Maher, "Oakland's Not for Burning? Popular Fury at Yet Another Police Murder," in *Raider Nation, Volume 1: From the January Rebellions to Lovelle Mixon and Beyond*, ed. Raider Nation Collective (Oakland: May 2010).

¹²⁹ Quoted in George Ciccariello-Maher, "'Oakland is Closed!' Arrest and Containment Fail to Blunt Anger in the Streets," in *Raider Nation, Volume 1: From the January Rebellions to Lovelle Mixon and Beyond*, ed. Raider Nation Collective (Oakland: May 2010) 20.

¹³⁰ It is worth noting how rarely the police are arrested for killing people on duty: In the U.S., it had

the mayor's office, no Justice Department investigation, and no arrests. In fact, the transit agency -- for whom Mehserle worked -- had not even interviewed him about the incident. This official silence provided the context for the riot.

"The rebellion on the seventh was not really about the murder," George Ciccariello-Maher explains. "The rebellion was really about the fact that nothing was being done." The riots produced political pressure, and got results. "If there's one lesson to take from this, it's that the only reason Mehserle was arrested is because people tore up the city. It was the riot -- and the threat of future riots."¹³¹

In an effort to re-assert its leadership, CAPE organized another demonstration for January 14. Speakers included Mayor Ron Dellums, the rapper Too \$hort, and representatives of various non-profits -- all of whom urged the crowd to remain peaceful. Furthermore, CAPE's designated marshals, operating under the supervision of a private security guard, surrounded the demonstration while unidentified informants mingled in the crowd to identify troublemakers.¹³²

Despite the tight control, things did not go as planned. When the speeches were over, much of the crowd refused to leave. Organizers announced that police would intervene if the group would not disperse; but rather than wait, CAPE's own marshals formed a line and began pushing people off the streets. The crowd -- now very angry -- started breaking windows. The security team, after consulting with police, withdrew and left it to the cops to handle the crowd. The police did what they do -- firing teargas and making arrests.¹³³

Future demonstrations, beginning on January 30, were handled accordingly -- with threats, arrests, and violence.¹³⁴

occurred only six times in the 15 years prior; and among the few prosecutions, Mehserle's was the only one to end in a conviction. Demian Bulwa, "Mehserle Convicted," *San Francisco Chronicle*, July 9, 2010.

¹³¹ George Ciccariello-Maher, "From Arizona to Oakland: The Intersections of Mass Work and Revolutionary Politics [Bring the Ruckus panel discussion]" (The Variant, Portland, Oregon; October 23, 2010).

¹³² Ciccariello-Maher, "Oakland is Closed," 22.

¹³³ Ciccariello-Maher, "Oakland is Closed," 23-26; Advance the Struggle, *Justice for Oscar Grant: A Lost Opportunity?* (2009) 5-8.

¹³⁴ Raider Nation Collective, "Introduction," in *Raider Nation, Volume 1: From the January Rebellions to Lovelle Mixon and Beyond*, ed. Raider Nation Collective (Oakland: May 2010) 5; and, George Ciccariello-Maher, "'Fired Up, Can't Take It No More': From Oakland to Santa Rita, The Struggle Continues," in *Raider Nation, Volume 1: From the January Rebellions to Lovelle Mixon and Beyond*, ed. Raider Nation Collective (Oakland: May 2010) 30-33.

"If we learned on January seventh that our power was in the streets," Ciccariello-Maher concludes, "what we learned on the fourteenth is that the state was going to counter-attack. . . . The state didn't counterattack by force at first; the state counter-attacked through these institutions, the nonprofits."¹³⁵

No Justice, Urban Peace

A year later, the process repeated itself. As Johannes Mehserle's trial approached, Nicole Lee, director of the non-profit "Urban Peace Movement," circulated an email focused, not on winning justice, but on preventing violence should justice be denied. Titled "Bracing for Mehserle Verdict: Community Engagement Plan," the June 23, 2010 memo offered two sets of instructions:

"1) Organizations, CBO's [Community-Based Organizations], and Public Agencies should be thinking of ways to *create organized events or avenues for young people and community members to express their frustrations with the system* in constructive and peaceful ways. If people have no outlets then it may be easier for folks to be pulled toward more destructive impulses.

2) We need to *begin 'inoculating' our bases and the community at-large so that when the verdict comes down, people are prepared* for it, and so that the 'outside agitators' who were active during the initial Oscar Grant protests are not able to incite the crowd so easily."¹³⁶

The memo goes on to list several talking points, which served the state's interests so well that the City of Oakland ran an edited version on its webpage.¹³⁷

Around the same time, another organization, ironically named "Youth Uprising,"

¹³⁵ Ciccariello-Maher, "From Arizona to Oakland."

¹³⁶ Reprinted in "Nonprofits Defend the State; Need More Proof?" *Advance the Struggle*, June 27, 2010, <http://advancethestruggle.wordpress.com/2010/06/27/nonpofits-defend-the-state-need-more-proof/#more-773>.

¹³⁷ Raider Nation Collective, "Lessons Never Learned: Nonprofits and the State, Redux," *Bring the Ruckus*, July 2, 2010, <http://bringtheruckus.org/?q=node/112>.

sponsored a public service announcement centered on the slogan, "Violence is Not Justice." The video includes local rappers, civil rights attorneys, school administrators, representatives from non-profits (including Nicole Lee), a police captain, and the District Attorney of San Francisco -- all urging a peaceful response to the verdict.¹³⁸ Religious leaders also got into the act, using the pulpit to ask people to remain safely at home when the verdict was announced.¹³⁹

The pacifying efforts, though broadly distributed, were centrally coordinated. Shortly before the trial, the Mayor and police held a meeting with several Bay Area non-profits. The topic, of course, was the prevention of riots.¹⁴⁰

In practice, avoiding unrest became the primary focus of the institutionalized left; CAPE's purported goal, the prevention of police brutality, receded into the background. If anything, by condemning the rioters and cooperating with the cops, liberal leaders helped to legitimize the police counter-attack and made further brutality more, not less, likely.

Mehserle was convicted, but of a lesser charge -- manslaughter, rather than murder. And, when the verdict was announced, rioting did ensue.¹⁴¹ Hundreds of people, mostly young people of color, braved not only the clubs and the tear gas of the police, but also the condemnation of their purported community leaders.

Advance the Struggle

In their published analysis of the Oscar Grant crisis, the revolutionary group Advance the Struggle argued that, by trying to de-fuse popular anger, "Bay Area nonprofits effectively acted as an extension of the state."¹⁴²

¹³⁸ Youth Uprising, "Violence Is Not Justice," YouTube.com, July 6, 2010, <http://www.youtube.com/watch?v=XqofgXqteuQ>.

The organization's website, YouthUprising.org presently quotes Attorney General Eric Holder, saying the group is a "perfect example of what we need to be doing around the country." YouthUprising.org. (Viewed October 14, 2010.)

¹³⁹ George Ciccariello-Maher, "Chronicle of a Riot Foretold," *CounterPunch*, June 29, 2010.

¹⁴⁰ Ciccariello-Maher, "Chronicle of a Riot Foretold."

¹⁴¹ George Ciccariello-Maher, "Oakland's Verdict," *CounterPunch*, July 12, 2010.

¹⁴² Advance the Struggle, *Justice for Oscar Grant*, 8-9.

For similar critiques of the role non-profits play in managing political struggle, see: *The Revolution Will Not Be Funded: Beyond the Non-Profit Industrial Complex*, ed. Incite! Women of Color Against Violence (Cambridge, Massachusetts: South End Press, 2007).

Had the rage over Grant's murder not been channeled into ritualized protest, had the leaders not been more interested in controlling the community response and preserving their own position than in confronting injustice, had the organizing not been, in a word, institutionalized -- it is hard to know what might have been possible.

Advance the Struggle contrasted the trajectory of events in Oakland with those of Greece, just a few weeks before the Grant killing:

"There, the police murder of a 15-year-old Alexandros Grigoropoulos triggered reactions which, very quickly, evolved from protests to riots to a general strike in which 2.5 million workers were on strike in December 2008. Within days the killer cop and police accomplices were arrested, but even this concession didn't trick the movement into subsiding. The police murder set off the uprising, but the participants connected the murder with the issues of unemployment, neo-liberal economic measures, political corruption, and a failing education system.

Aren't we facing similar problems in Oakland . . . ?"¹⁴³

Of course there are differences between Oakland and Athens -- differences of geography, history, and political culture. The type of insurrection unleashed in Greece may not, at present, be possible in California. But rather than being an *objection* to the radical analysis, this is precisely *the point*. The political environment in Oakland has been shaped in such a way so as to sharply limit the possibilities of struggle. And the institutionalization of conflict in professionalized nonprofits is an important part of that restrictive context. There is no guarantee that things would have gone further had the nonprofits not intervened, or that greater conflict would have won greater gains. But their intervention certainly helped to contain the rebellion, and closed off untold possibilities for further action. That is, quite clearly, what it was intended to do.

¹⁴³ Advance the Struggle, *Justice for Oscar Grant*, 22. Paragraph break added for emphasis.

The cop who shot Grigoropoulos was convicted and sentenced to life in prison. Another cop was convicted as an accomplice, and sentenced to ten years. Associate Press, "Greece: Police Officer Convicted in Killing That Led to Riots," *New York Times*, October 11, 2010.

Conclusion: Countering Counterinsurgency; Lessons for Social Movements

Insurgent Thinking

When facing counterinsurgency, we need to learn to think like insurgents.

We have to recognize, and even embrace, political and strategic complexity. Every insurgency is different, and a single insurgency may take very different forms from one year to the next, or one street to the next. There are no set paths or ready formulas, which is not the same thing as saying there are no strategies. But our strategies have to correspond with the reality we face, not with an idealized version of some past revolution or some future utopia. And we cannot elevate our own favorite tactics -- whether pacifist or insurrectionist -- into articles of faith.

The Limits of Security Culture

As this suggests, there are no technical solutions to the problem of repression.

The common activist conception of "security culture" is really little more than a cult of secrecy. The numerous handbooks and zines on the subject prescribe specific techniques to avoid *getting caught*, but they are generally silent about all the other dynamics of resistance and repression. Their advice applies to clandestine, illegal, militant action, but typically says nothing about the measures necessary to protect legal, non-violent, above-ground activity (which is, after all, the largest portion of political work). Worse, by relying entirely on evasion and secrecy, this approach too often separates militant action -- sometimes even the militants themselves -- from the rest of the movement. This can create an imbalance, and tension, between militant tactics and popular legitimacy. And it can leave the militants isolated from any base of support, and thus increasingly vulnerable to repression. It is this sort of isolation, along with sharp divisions within the anarchist movement, that allowed the FBI to convert militants into informants during Operation Backfire.¹⁴⁴

¹⁴⁴ "Green Scared?" *Rolling Thunder*, 31-2.

On the other hand, in liberal circles it is sometimes thought that if we stay within the law, the state will *also* stay within the law, respecting our right to peacefully dissent; and, should the cops overstep their bounds and interfere with our lawful political activity, we can seek relief from the courts. The long history of repression against legal political action suggests the limits to this approach.¹⁴⁵ It is true that, at times, the state shows greater tolerance to dissent when it appears in its law-abiding, non-violent, institutionalized form. But as we have seen, that tolerance is premised on the contained and controlled nature of the opposition. Dissent is tolerated only until it begins to interfere with the normal operations of power.

Both the clandestine and the civil-liberties approach to security, for different reasons, assume an overall framework of legality and treat repression as a criminal-justice problem. But social movements are targeted according to the political threat they present, not because of the laws they break. The state's first imperative is to defend its own ability to rule; legality and peace are secondary, at best.

So, when activists come under attack, legal defenses -- the kind that rely on lawyers and court rulings -- will not be enough; a political defense is also required. Therefore we need to move beyond legal narratives of guilt or innocence and employ political narratives of struggle and repression. That means, when it comes to accusations of sabotage, rioting, and other political crimes, we need to be prepared to support the guilty along with innocent. It also means that we need to build public support, both for particular tactics and for the objectives they are meant to advance.¹⁴⁶ And, perhaps most importantly, social movements need to facilitate the community's ability to act on its own initiative.

The Best Defense

The antidote to repression is *more resistance*. But this can't just be a matter of

¹⁴⁵ Jules Boykoff, *Beyond Bullets: The Suppression of Dissent in the United States* (Oakland: AK Press, 2007).

¹⁴⁶ Howard Zinn observes, "One sign that the ideas of the antiwar movement had taken hold in the American public was that juries became more reluctant to convict antiwar protestors, and local judges were dismissing charges against demonstrators in cases where two years before they almost certainly would have been sent to jail." Howard Zinn, *A People's History of the United States, 1492-Present* (New York: HarperPerennial, 1995) 491.

escalating tactics or increasing militancy; crucially, it has to involve broadening the base of support. Solidarity is the key to our strength, and the source of our security.

Again, repression is not simply a legal or a military exercise, but rather it employs legal and military elements in the service of a political campaign. Countering repression requires that we, too, keep the political question in the forefront and, more particularly, politicize and problematize the state's use of violence and the courts. We have to make repression a problem for the state.

One approach is to use the government's strength against it:

"the domestic use of force by the state has an inherent potential to weaken its own ultimate bulwark: legitimacy. This is especially the case in countries where state security services have a history of brutalizing the people on behalf of the regime. . . . [T]he risk of strengthening insurgency by damaging legitimacy is especially high if (1) the insurgency is embedded in the population, (2) the insurgency already enjoys some popular sympathy, (3) force is not used with great care, or (4) foreign troops use force on the state's behalf. Some such potential is inherent in all COIN because of the risk that deadly force and intimidation will so alienate the population that its support for the insurgency rises and that recruiting outpaces losses."¹⁴⁷

The best defense is a good offense: Whatever the issue or the ultimate aims, social movements need to build in demands for freedom of speech, freedom of assembly, and the rest. Moreover, our movements need to actively push for limits on police power -- restrictions on surveillance, regulations concerning the files they can keep, civilian oversight, and so on. And in particular, we need to present the limits to police action in terms of generalizable rights, not as special privileges enjoyed by activists. It is short-sighted and unprincipled to allow for "gang enforcement teams" while objecting to red

¹⁴⁷ Gompert and Gordon, *War by Other Means*, 63.

For a case study drawn from U.S. history, see: Mark Grimsley, "Why the Civil Rights Movement was an Insurgency," *HistoryNet.com*, [2010], <http://www.historynet.com/why-the-civil-rights-movement-was-an-insurgency.htm>.

squads. Counterinsurgency preempts political opposition by targeting the communities most likely to resist; insurgents need to defend those communities, for the same reason.

This requires something more than a standard "civil liberties" agenda. It requires an aggressive attack against the institutions of power. It is not enough to oppose political policing, political surveillance, and political prisons; we need to learn to see *all* policing, surveillance, and prisons as political, and oppose them accordingly. That is -- we should not only fight against particular policies or practices, but against the institutions *themselves*. We must seek to constrain, restrict, and ultimately dismantle the apparatus of repression. And we must simultaneously attack the system of power it represents, and the fundamental inequalities -- those of race, class, gender, and nationality -- it seeks to preserve.

Politics First

Above all, that we have to pursue a strategy of struggle rather than accommodation with the existing system. Frederick Douglass knew what he was talking about: "Power concedes nothing without a demand."¹⁴⁸ Rights are not *given*, they are *won*. And the authorities only offer concessions when they feel that their power is threatened.

Those concessions can -- indeed, are often meant to -- undermine the very movement that made reforms possible, and therefore undercut the possibility of further change.¹⁴⁹ Reforms can be used to divide moderates from extremists, reduce the sense of urgency, demobilize the constituency, and re-align the population with the authorities. Therefore, we have to be strategic in making demands, forwarding proposals that open, rather than close, the possibilities for further action. We also have to be careful to avoid the institutionalization of struggle, the co-optation of our organizations and leaders, the channeling of conflict into forms that can be incorporated into the existing system and managed without a shift in power.¹⁵⁰

¹⁴⁸ Quoted in Frederic May Holland, *Frederick Douglass: The Colored Orator* (New York: Funk and Wagnalls Company, 1891), 261.

¹⁴⁹ Galula is explicit on this point, and offers detailed advice on offering reforms. Galula 103.

¹⁵⁰ As Galula notes, "a good cause for the insurgent is one that his opponent cannot adopt without losing his power in the process." Galula, *Counter-Insurgency Warfare*, 67.

Legality and nonviolence do not, on their own, do anything to protect us from repression. On the other hand, militancy, alone, may produce heroes or martyrs, but not revolution. We have to remember that an insurgency is not just a series of tactical exchanges with the state. It is, instead, a contest for the support of the population: “*Legitimacy is the main objective.*”¹⁵¹ The primary struggle is political.

Bio

Kristian Williams is the author of *Our Enemies in Blue: Police and Power in America* and *American Methods: Torture and the Logic of Domination* (both from South End Press). He is a member of Rose City Copwatch, in Portland, Oregon.

¹⁵¹ FM 3-24, 1-113.

Art of Intrusion

- 1- How do social engineering attacks use small pieces of information to build credibility? What does that suggest in terms of sharing information? How much secrecy is necessary, or practical?
- 2- What does this article suggest in terms of using casual cues to build trust? How does your organization decide whom to trust?
- 3- Discuss the countermeasures listed on page 238. Explain what you understand them to consist of and how they relate to your organization's work. Relate them to Schneier's five questions.

Pseudo Ops

- 1- What are the defining features of a pseudo-op? How do pseudo ops differ from normal infiltration? How could pseudo-ops be employed outside the guerilla warfare context?
- 2- What organizational or social movement vulnerabilities do pseudo ops exploit? How are these vulnerabilities similar to those exploited in social engineering attacks? Do you see similar vulnerabilities in the movement of which you are a part? Could these vulnerabilities be corrected?
- 3- Can a pseudo op be recognized from the outside? How? How can pseudo-groups be distinguished from genuine organizations who behave irresponsibly, or with which you happen to disagree?
- 4- Review each of Cline's six "Lessons Learned." What corresponding lessons do they suggest for social movements?
- 5- Review the "Programs for Countering Social Engineering" from The Art of Intrusion. Could these principles help counter pseudo-ops? Can you think of others? How does your organization employ these procedures?

Chapter 10

Social Engineers — How They Work and How to Stop Them

The social engineer employs the same persuasive techniques the rest of us use every day. We take on roles. We try to build credibility. We call in reciprocal obligations. But the social engineer applies these techniques in a manipulative, deceptive, highly unethical manner, often to devastating effect.

— Social Psychologist Dr. Brad Sagarin

This chapter does something a bit different: We look at the most difficult type of attack to detect and defend against. The social engineer, or the attacker skilled in the art of deception as one of the weapons in his or her toolkit, preys on the best qualities of human nature: our natural tendencies to be helpful, polite, supportive, a team player, and the desire to get the job done.

As with most things in life that threaten us, the first step toward a sensible defense is understanding the methodologies used by cyber-adversaries. So, we present here a set of psychological insights that probe the underpinnings of human behavior allowing the social engineer to be so influencing.

First, though, an eye-opening story of a social engineer at work. The following is based on a story we received in writing that is both amusing and a textbook case of social engineering. We thought it so good that we have included it despite some reservations; the man either had accidentally

omitted some of the details because he was distracted on other business matters or else he made up portions of the story. Still, even if some of this is fiction, it makes the case very convincingly of the need for better protection against social engineering attacks.

As elsewhere throughout the book, details have been changed to protect both the attacker and the client company.

A SOCIAL ENGINEER AT WORK

In the summer of 2002, a security consultant whose handle is “Whurley” was hired by a resort group in Las Vegas to perform a variety of security audits. They were in the process of reengineering their approach to security and hired him to “try to circumvent any and all processes” in an effort to help them build a better security infrastructure. He had plenty of technical experience, but little experience being in a casino.

After a week or so of immersing himself in research on the culture of the Strip, it was time for the real Las Vegas. He usually made it a practice to start a job like this early, getting finished before it was officially scheduled to begin, because over the years he had found that managers don’t tell employees about a potential audit until the week they think it’s going to happen. “Even though they shouldn’t give anyone a heads up, they do.” But he easily circumvented this by performing the audit in the two weeks before the scheduled date.

Though it was nine at night by the time he arrived and settled into his hotel room, Whurley went straight to the first casino on his list to start his on-site research. Having not spent a lot of time in casinos, this experience was quite an eye-opener for him. The first thing he noticed contradicted what he had seen on the Travel channel, where every casino staffer shown or interviewed appeared to be an elite security specialist. The majority of the employees he watched on-site seemed to be “either dead asleep on their feet or completely complacent in their job.” Both of these conditions would make them easy targets for the simplest of confidence games — which wasn’t even going to come close to what he had planned.

He approached one very relaxed employee and with a very little prodding found the person willing to discuss the details of his job. Ironically, he had previously been employed by Whurley’s client-casino. “So, I bet that was a lot better, huh?” Whurley asked.

The employee replied, “Not really. Here I get floor-audited all the time. Over there they hardly noticed if I was a little behind, pretty much

that way for everything . . . time clocks, badges, schedules, whatever. Their right hand doesn't know what their left is doing."

The man also explained that he used to lose his employee badge all the time, and sometimes he would just share a badge with another employee to get in for the free meals provided to employees in the staff cafeterias located within the bowels of the casino.

The next morning Whurley formulated his goal, which was straightforward — he would get into every protected area of the casino that he could, document his presence, and try to penetrate as many of the security systems as he could. In addition, he wanted to find out if he could gain access to any of the systems that ran the financials or held other sensitive information, such as visitor information.

That night, on the way back to his hotel after visiting the target casino, he heard a promotion on the radio for a fitness club offering a special for service industry employees. He got some sleep and the next morning headed for the fitness club.

At the club, he targeted a lady named Lenore. "In 15 minutes we had established a 'spiritual connection.'" This turned out to be great because Lenore was a financial auditor and he wanted to know everything that had to do with the words "financial" and "audit" at the target casino. If he could penetrate the financial systems in his audit, it was sure to be viewed as a huge security flaw by the client.

One of Whurley's favorite tricks to use when he's social engineering is the art of cold reading. As they were talking, he would observe her non-verbal signals and then throw out something that would lead her to say, "Oh, no shit — me, too." They hit it off, and he asked her out to dinner.

Over dinner, Whurley told her that he was new to Vegas and looking for a job, that he had gone to major university and had a degree in Finance, but that he had moved to Vegas after breaking up with his girlfriend. The change of pace would help him get over the breakup. Then he confessed to being a little intimidated by trying to get an auditing job in Vegas because he didn't want to end up "swimming with the sharks." She spent the next couple of hours reassuring him that he would not have a hard time getting a finance job. To help out, Lenore provided him with more details about her job and her employer than he even needed. "She was the greatest thing that had happened to me so far on this gig, and I gladly paid for dinner — which I was going to expense anyway."

Looking back, he said that at this point he was overconfident about his abilities, "which cost me later." It was time to get started. He had packed a

bag with “a few goodies including my laptop, an Orinoco broadband wireless gateway, an antenna, and a few other accessories.” The goal was simple. Try to get into the office area of the casino, take some digital photos (with time stamps) of himself in places he shouldn’t be, and then install a wireless access point on the network so that he could try to remotely hack into their systems to collect sensitive information. To complete the job, the next day he would have to go back in to get the wireless access point.

“I was feeling quite like James Bond.” Whurley arrived at the casino, outside the employee’s entrance, right at the shift change, positioning himself to be able to observe the entrance. He thought he would be there in time to observe things for a few minutes, but most of the people seemed to have arrived already and he was stuck trying to walk in all by himself.

A few minutes of waiting and the entryway was clear . . . which was not what he wanted. Whurley did, however, notice a guard who looked as if he were leaving but was stopped by a second guard and they stood around smoking just outside the exit. When they finished their cigarettes, they parted and started walking in opposite directions.

I headed across the street towards the guard who was leaving the building and prepared to use my favorite disarming question. As he approached me crossing the street, I let him get just past me.

Then he said, “Excuse me, excuse me, do you have the time?”

It was by plan. “One thing I’ve noticed is that if you approach someone from the front, they’re almost always more defensive than if you let them get slightly past you before you address them.” While the guard was telling Whurley the time, Whurley was looking him over in detail. A name badge identified the guard as Charlie. “As we were standing there, I had a stroke of luck. Another employee came walking out and called Charlie by his nickname, Cheesy. So I asked Charlie if he caught shit like that a lot and he told me how he got the nickname.”

Whurley then headed toward the employee entrance at a quick pace. It’s often said that the best defense is a good offense, and that was his plan. As he reached the entrance, where he had noticed employees showing their badges earlier, he went straight up to the guard at the desk and said, “Hey, have you seen Cheesy? He owes me \$20 on the game and I need the money to get some lunch when I go on break.”

Recalling that moment, he says, “Damn! This is where I got my first challenge.” He had forgotten that employees get their meals free. But he

wasn't put off by being challenged; while others with attention deficit/hyperactivity disorder (ADHD) might see it as a problem, Whurley describes himself as "very ADHD," and adds that, as a result, "I can think much faster on my feet than 90 percent of the people I run into." That ability came in handy here.

So the guard says, "What the hell are you buying lunch for anyway?" and chuckled but started looking suspicious. Quickly I threw out, "I'm meeting a little honey for lunch. Man, she's hot. (This always distracts older guys, out of shape guys, and the living-with-mom type guys.)" "What am I going to do?"

The guard says, "Well, you're screwed 'cause Cheesy's gone for the rest of the week."

"Bastard!" I say.

The guard then amused Whurley (an amusement he didn't dare show) by unexpectedly asking if he was in love.

I just start rolling with it. Then I got the surprise of my life. I have never even come close to something like this. It could be attributed to skill, but I rack it up to blind luck: the guy gives me \$40! He tells me \$20 won't buy shit and I obviously need to be the one that pays. Then he gives me five minutes of "fatherly" advice, and all about how he wished he had known what he knows now when he was my age.

Whurley was "in awe" that the guy bought this con and was paying for his imaginary date.

But, things weren't going as smoothly as Whurley thought, because as he started walking off, the guard realized he hadn't shown any ID and challenged him. "So I said, 'It's in my bag, sorry about that' and started digging through my stuff as I proceeded away from him. That was a close call 'cause if he'd have insisted on seeing the ID, I might have been screwed."

Whurley was now inside the employee entrance but had no idea where to go. There weren't a lot of people he could follow, so he just walked with confidence and started taking mental notes of his surroundings. He had little fear of being challenged at this point. "Funny," he said, "how the psychology of color can come in so handy. I was wearing blue — the truth color — and dressed as if I were a junior executive. Most of the people running around were wearing staffer clothes, so it was highly unlikely they would question me."

As he was walking down the hallway, he noticed that one of the camera rooms just looked just like the ones he had seen on the Travel Channel — an “Eye in the Sky” room, except that this one wasn’t overhead. The outer room had “the most VCRs I had ever seen in one place — wow, was it cool!” He walked through to the inner room and then did something especially gutsy. “I just walked in, cleared my throat and before they could challenge me, I said, ‘Focus on the girl on 23.’”

All the displays were numbered, and, of course, there was a girl on nearly every one. The men gathered around display 23 and they all began talking about what the girl might be up to, which Whurley thought generated a good deal of paranoia. This went on for some 15 minutes just checking out people on monitors, with Whurley deciding that the job is a perfect one for anyone with a propensity for voyeurism.

As he was getting ready to leave, he announced, “Oh, I got so caught up in that action, I forgot to introduce myself. I’m Walter with Internal Audit. I just got hired onto Dan Moore’s staff,” using the name of the head of Internal Audit that he had picked up in one of his conversations. “And I’ve never been to this property so I’m a little lost. Could you point me in the direction of the executive offices?”

The guys were more than happy to get rid of an interfering executive and eager to help “Walter” find the offices he was looking for. Whurley set out in the direction they indicated. Seeing nobody in sight, he decided to take a look around and found a small break room where a young woman was reading a magazine. “She was Megan, a real nice girl. So Megan and I talked for a few minutes. Then she says, ‘Oh, if you’re with Internal Audit, I have some stuff that needs to go to back there.’” As it turned out, Megan had a couple of badges, some internal memos, and a box of papers that belonged back at the main resort group Internal Audit office. Whurley thought, “Wow, now I have a badge!”

Not that people look at the pictures on ID badges very carefully, but he took the precaution of flipping it around so only the back was visible.

As I’m walking out, I see an open, empty office. It has two network ports, but I can’t tell if they’re hot by just looking at them, so I go back to where Megan is sitting and tell her that I forgot I was supposed to look at her system and the one in “the boss’s office.” She graciously agrees and lets me sit at her desk.

She gives me her password when I ask, and then has to use the restroom. So, I tell her I’m going to add a “network security monitor” and show her the wireless access point. She replies, “Whatever. I don’t really know much about that geeky stuff.”

While she was out, he installed the wireless access point and restarted her desktop. Then he realized he had a 256MB universal serial bus (USB) flash drive on his key chain and full access to Megan's computer. "I start surfing through her hard drive and find all kind of good stuff." It turned out that she was the executive administrator for every one of the executives and that she had organized their files by name "all nice and neat." He grabbed everything he could, then, using the timer feature on his digital camera, took a picture of himself sitting in the main executive's office. After a few minutes Megan returned, and he asked her for directions to the Network Operations Center (NOC).

There he ran into "serious trouble." He said, "First off, the network room was marked . . . which was cool. However, the door is locked." He didn't have a badge that would give him access and tried knocking.

A gentleman comes to the door and I tell him the same story I've been using: "Hi, I'm Walter with Internal Audit and blah, blah, blah." Except what I don't know is that this guy's boss — the IT director — is sitting in the office. So the guy at the door says "Well, I need to check with Richard. Wait here a second."

He turns around and tells another guy to get Richard and let him know that there is someone "claiming" to be from Internal Audit at the door. A few moments later, I get busted. Richard asks who I'm with, where my badge is, and a half dozen other questions in rapid succession. He then says, "Why don't you come into my office while I call Internal Audit and we'll get this cleared up."

Whurley figured that "This guy has totally busted me." But then, "Thinking quickly, I tell him 'You got me!' and I shake his hand. I then tell him 'My name is Whurley.' And I reach in my bag for a business card. I then tell him that I've been down inside the bowels of the casino for a couple of hours and not one person has challenged me, and that he was the first and was probably going to look pretty good in my report. I then say, 'Let's go sit in your office while you call over so you know everything is legitimate. Besides,' I say, 'I need to go ahead and tell Martha, who is in charge of this operation, about a couple of the things I've seen down here.'"

For an on-the-spot gambit in a tight situation, it turned out to be brilliant. An amazing transformation took place. Richard began asking Whurley about what he had seen, people's names, and so on, and then explained that he had been doing his own audit in an attempt to get an increase in the security budget to make the NOC more secure, with "biometrics and

the whole works.” And he suggested that maybe he could use some of Whurley’s information to help him achieve his goal.

By then it was lunch time. Whurley took advantage of the opening by suggesting that maybe they could talk about it over lunch, which Richard seemed to think was a good idea, and they headed off together to the staff cafeteria. “Notice that we haven’t called anyone yet at this point. So I suggest that we place that call, and he says, ‘You’ve got a card, I know who you are.’” So the two ate together in the cafeteria, where Whurley got a free meal and made a new “friend.”

“He asked about my networking background and we started talking about the AS400s that the casino is running everything on. The fact that things went this way can be described in two words — very scary.” Scary because the man is the director of IT, and responsible for computer security, is sharing all kinds of privileged, inside information with Whurley but has never taken the most basic step of verifying his identity.

Commenting on this, Whurley observed that “mid-level managers don’t ever want to be put ‘on the spot.’ Like most of us, they never want to be wrong or get caught making an obvious mistake. Understanding their mindset can be a huge advantage.” After lunch, Richard brought Whurley back to the NOC.

“When we walk in, he introduces me to Larry, the main systems administrator for the AS400s. He explains to Larry that I’m going to be ‘ripping’ them in an audit in a few days, and he had had lunch with me and got me to agree to do a preliminary audit and save them any major embarrassment” when it came time for the actual audit. Whurley then spent a few minutes getting an overview of the systems from Larry, gathering more useful information for his report; for example, that the NOC stored and processed all of the aggregate data for the entire resort group.

I told him that it would help me to help him faster if I had a network diagram, firewall Access Control Lists, and so on, which he provided only after calling Richard for approval. I thought, “Good for him.”

Whurley suddenly realized that he had left the wireless access point back in the executive offices. Though the chances that he would be caught had dropped dramatically since establishing his rapport with Richard, he explained to Larry that he needed to go back to get the access point he had left. “To do this I would need a badge so I could let myself back into the NOC and come and go as I pleased.” Larry seemed a bit reluctant to do this, so Whurley recommended that he call Richard

again. He called and told Richard that the visitor wanted to be issued a badge; Richard had an even better idea: The casino had recently let several employees go, and their badges were in the NOC and nobody had found the time yet to deactivate them, “so it would be all right for him to just use one of those.”

Whurley went back to having Larry explain the systems and describe the security measures they had recently taken. A phone call came in from Larry’s wife, apparently angry and upset about some ongoing issue. Whurley pounced on this volatile situation, recognizing he could benefit. Larry said to his wife, “Listen, I can’t talk. I have someone here in the office.” Whurley motioned for Larry to put his wife on hold for a second and then offered advice about how important it was for him to work through the problem with her. And he offered to grab one of the badges if Larry would show him where they were.

“So Larry walked me over to a filing cabinet, opened a drawer, and just said ‘Take one of these.’ He then walked back to his desk and picked up the phone. I noticed that there was no sign-out sheet or log of the badge numbers, so I took two of the several that were there.” He now had not just a badge, but one that would allow him access to the NOC at any time.

Whurley then headed back to see his new friend Megan, recover his wireless access point, and see what else he could find out. And he could take his time about it.

I figured the time wouldn’t really matter because he’d be on the phone with his wife and he’d stay distracted for longer than he thought. I set the stopwatch on my phone to count down twenty minutes, enough time for me to do some exploring without drawing additional suspicion from Larry, who appeared to suspect something was up.

Anyone who’s ever worked in an IT department knows that ID badges are tied to a computer system; with the right PC access, you can expand your access to go anywhere in the building. Whurley was hoping to discover the computer where badge access privileges were controlled so he could modify the access on the two badges he had. He walked through the corridors looking into offices for the control system for the badges, which proved to be harder than he thought. He felt frustrated and stumped.

He decided to ask someone and settled on the guard who had been so friendly at the employees’ entrance. By now many people had seen him with Richard, so that suspicions were almost nonexistent. Whurley found

his mark and told him that he needed to see the building access control system. The guard didn't even ask why. No trouble. He was told exactly where to find what he was looking for.

"I located the control system and walked into the small networking closet where it was located. There I found a PC on the floor with the list for the ID badges already open. No screen saver, no password — nothing to slow me down." In his view, this was typical. "People have an 'out of sight, out of mind' mentality. If a system like this is in a controlled access area, they think there isn't any need to be diligent about protecting the computer."

In addition to giving himself all-areas access, there was one more thing he wanted to do:

Just for fun, I thought I should take the extra badge, add some access privileges, switch the name, and then switch it with an employee who would be wandering around the casino, inadvertently helping me to muddy the audit logs. But who would I choose? Why Megan, of course — it would be easy to switch the badges with her. All I would have to do is tell her I needed her help with the audit.

When Whurley walked in, Megan was as friendly as ever. He explained that he had completed the test and needed to get that equipment back. He then told Megan that he needed her help. "Most social engineers would agree that people are too willing to help." He needed to see Megan's badge to check it against the list he had. A few moments later, Megan had a badge that would confuse things even further, while Whurley had her badge as well as the badge that would tag him as an executive in the logs.

When Whurley got back to Larry's office, the distraught manager was just finishing the call with his wife. Finally hanging up, he was ready to continue their conversation. Whurley asked that the network diagrams be explained in detail to him, but then interrupted and, to disarm him, Whurley asked about how things were going with Larry's wife. The two men spent almost an hour talking about marriage and other life issues.

At the end of our talk, I was convinced that Larry wouldn't be causing me any more issues. So, now I explain to Larry that my laptop has special auditing software I need to run against the network. Since I usually have top gear, getting the laptop hooked up to the network is always easy because there isn't a geek on the planet who doesn't want to see it running.

After a while, Larry stepped away to make some phone calls and attend to other items. Left to himself, Whurley scanned the network and was able to compromise several systems, both Windows and Linux machines, because of poor password management, and then spent nearly two hours starting and stopping copies of information off the network and even burning some of the items to DVD, “which was never questioned.”

After completing all of this I thought it would be funny, and useful, to try one more thing. I went to every individual that I had come in contact with — and some that had just briefly seen me with others — and told them some variant of “Well, I’m done. Say, could you do me a favor. I like to collect pictures of all the people and places I work at. Would you mind taking a picture with me?” This proved to be “amazingly simple.”

Several people even offered to take the pictures of him with others in nearby offices. He had also secured badges, network diagrams, and access to the casino’s network. And he had photos to prove it all.

At the review meeting, the head of Internal Audit complained that Whurley had no right to try to access the systems in a physical way because “that wasn’t how they would be attacked.” Whurley was also told that what he did bordered on “criminal” and that the client didn’t at all appreciate his actions.

Whurley explained:

Why did the casino think that what I did was unfair? The answer was simple. I had not worked with any casino before and did not fully understand the regulations [they operate under]. My report could cause them to be audited by the Gaming Commission, which could potentially have actual financial repercussions.

Whurley was paid in full, so he didn’t mind very much. He wished that he had left a better impression on the client but felt they pretty much hated the approach he had used and thought it unfair to them and to their employees. “They made it very clear that they didn’t really want to see me around anymore.”

That hadn’t happened to him before; usually clients appreciated the results of his audits and saw them as what he called “mini-red teaming events or War Games,” meaning they were okay with being tested using the same methods that a hostile hacker or social engineer might. “Clients almost always get a thrill out of it. I had, too, until this point in my career.”

All in all, Whurley rates this Vegas experience as a success in the area of testing, but a disaster in the area of client relations. “I’ll probably never work in Vegas again,” he laments.

But then, maybe the Gaming Commission needs the consulting services of an ethical hacker who already knows his way around the back areas of a casino.

INSIGHT

Social psychologist Brad Sagarin, PhD, who has made a study of persuasion, describes the social engineer’s arsenal this way: “There’s nothing magic about social engineering. The social engineer employs the same persuasive techniques the rest of us use every day. We take on roles. We try to build credibility. We call in reciprocal obligations. But unlike most of us, the social engineer applies these techniques in a manipulative, deceptive, highly unethical manner, often to devastating effect.”

We asked Dr. Sagarin to provide descriptions of the psychological principles underlying the most common tactics used by social engineers. In a number of cases, he accompanied his explanation with an example from the stories in the earlier Mitnick/Simon book, *The Art of Deception* (Wiley Publishing, Inc., 2002), that illustrated the particular tactic.

Each item begins with an informal, nonscientific explanation of the principle, and an example.

Trappings of Role

The social engineer exhibits a few behavioral characteristics of the role he or she is masquerading in. Most of us tend to fill in the blanks when given just a few characteristics of a role — we see a man dressed like an executive and assume he’s smart, focused, and reliable.

Example: When Whurley entered the Eye in the Sky room, he was dressed like an executive, he spoke with a commanding authority, and he gave what the men in the room took to be an order to action. He had successfully donned the trappings of a casino manager or executive.

In virtually every social engineering attack, the attacker uses trappings of role so the target will infer other characteristics of the role and act accordingly. The role may be as an IT technician, a customer, a new hire, or any of many others that would ordinarily encourage compliance with a request. Common trappings include mentioning the name of the target’s boss or

other employees, or using company or industry terminology or jargon. For in-person attacks, the attacker's choice of clothing, jewelry (a company pin, an athlete's wristwatch, an expensive pen, a school ring), or grooming (for example, hairstyle) are also trappings that can suggest believability in the role that the attacker is claiming. The power of this method grows from the fact that once we accept someone (as an executive, a customer, a fellow employee), we make inferences attributing other characteristics (an executive is wealthy and powerful, a software developer is technically savvy but may be socially awkward, a fellow employee is trustworthy).

How much information is needed before people start making these inferences? Not much.

Credibility

Establishing credibility is step one in most social engineering attacks, a cornerstone for everything that is to follow.

Example: Whurley suggested to Richard, a senior IT person, that the two of them have lunch together, realizing that his being seen with Richard would immediately establish his credibility with any employee who noticed them together.

Dr. Sagarin identified three methods used in *The Art of Deception* that social engineers rely on to build credibility. In one method, the attacker says something that would seem to be arguing against his or her self-interest, as found in Chapter 8 of *The Art of Deception* in the story “One Simple Call,” when the attacker tells his victim, “Now, go ahead and type your password but don’t tell me what it is. You should never tell anybody your password, not even tech support.” This sounds like a statement from someone who is trustworthy.

In the second method, the attacker warns the target of an event that (unknown to the target) the attacker causes to occur. For example, in the story, “The Network Outage,” appearing in Chapter 5 of *The Art of Deception*, the attacker explains that the network connection might go down. The attacker then does something that makes the victim lose his network connection, giving the attacker credibility in the eyes of the victim.

This prediction tactic is often combined with the third of these methods, in which the attacker further “proves” he or she is credible by helping the victim solve a problem. That’s what happened in “The Network Outage,” when the attacker first warned that the network might go out, then caused the victim’s network connection to fail, as predicted, and subsequently restored the connection and claimed that he had “fixed the problem,” leaving his victim both trusting and grateful.

Forcing the Target into a Role (Altercasting)

The social engineer maneuvers his or her target into an alternative role, such as forcing submission by being aggressive.

Example: Whurley, in his conversations with Lenore, put himself into a needy role (just broke up with his girlfriend, just moved to town and needs a job), in order to maneuver her into a helper role.

In its most common form, the social engineer puts his or her target into the role of helper. Once a person has accepted the helper role, he or she will usually find it awkward or difficult to back off from helping.

An astute social engineer will try to gain a sense of a role that the victim would be comfortable in. The social engineer will then manipulate the conversation to maneuver the person into that role — as Whurley did with both Lenore and Megan when he sensed they would be comfortable as helpers. People are likely to accept roles that are positive and that make them feel good.

Distracting from Systematic Thinking

Social psychologists have determined that human beings process incoming information in one of two modes, which they have labeled the systematic and the heuristic.

Example: When a manager needed to handle a difficult situation with his distraught wife, Whurley took advantage of the man's emotional state and distraction to make a request that landed him an authentic employee's badge.

Dr. Sagarin explains, “When processing systematically, we think carefully and rationally about a request before making a decision. When processing heuristically, on the other hand, we take mental shortcuts in making decisions. For example, we might comply with a request based on who the requestor claims to be, rather than the sensitivity of the information he or she has requested. We try to operate in the systematic mode when the subject matter is important to us. But time pressure, distraction, or strong emotion can switch us to the heuristic mode.”

We like to think that we normally operate in a rational, logical mode, making decisions based on the facts. Psychologist Dr. Gregory Neidert has been quoted as saying, “we humans are running our brains at idle about 90 percent to 95 percent of the time.”¹ Social engineers try to take advantage of this, using a variety of influence methods to force their victims to shift out of the systematic mode — knowing that people operating in a heuristic mode are much less likely to have access to their

psychological defenses; they are less likely to be suspicious, ask questions, or present objections to the attacker.

Social engineers want to approach targets that are in heuristic mode and keep them there. One tactic is to call a target five minutes before the end of the workday, counting on the fact that anxiety about leaving the office on time may lead the target to comply with a request that might otherwise have been challenged.

Momentum of Compliance

Social engineers create a momentum of compliance by making a series of requests, starting with innocuous ones.

Example: Dr. Sagarin cites the story “CreditChex,” appearing in Chapter 1 of The Art of Deception, in which the attacker buries the key question, sensitive information about the bank’s Merchant ID number, which was used as a password to verify identity over the phone, in the middle of a series of innocuous questions. Since the initial questions appear to be innocuous, this establishes a framework in which the victim is positioned to treat the more sensitive information as also innocuous.

Television writer/producer Richard Levinson made this a tactic of his most famous character, Columbo, played by Peter Falk. Audiences delighted in knowing that just as the detective was walking away, and the suspect was lowering his or her defenses, pleased with themselves at fooling the detective, Columbo would stop to ask one final question, the key question that he had been building up to all along. Social engineers frequently make use of this “one-more-thing” tactic.

The Desire to Help

Psychologists have identified many benefits people receive when they help others. Helping can make us feel empowered. It can get us out of a bad mood. It can make us feel good about ourselves. Social engineers find many ways of taking advantage of our inclination to be helpful.

Example: When Whurley showed up at the employees’ entrance of the casino, the guard believed his story about taking a “honey” to lunch, loaned him money for the date, gave him advice about how to handle a woman, and didn’t become insistent when Whurley walked away without ever having shown an employee’s ID badge.

Dr. Sagarin comments, “Because social engineers often target people who don’t know the value of the information they are giving away, the help may be seen as carrying little cost to the helper. (How much work

is it to do a quick database query for the poor slob on the other end of the telephone?)”

Attribution

Attribution refers to the way people explain their own behavior and that of others. A goal of the social engineer is to have the target attribute certain characteristics to him or her, such as expertise, trustworthiness, credibility, or likability.

Example: Dr. Sagarin cites the story, “The Promotion Seeker,” appearing in Chapter 10 of The Art of Deception. The attacker hangs around for a while before requesting access to a conference room, allaying suspicion because people assume an intruder wouldn’t dare spend time unnecessarily in a place where he or she might be caught.

A social engineer might walk up to a lobby receptionist, put a \$5 bill down on the counter, and say something like, “I found this on the floor. Did anyone say they lost some money?” The receptionist would attribute to the social engineer the qualities of honesty and trustworthiness.

If we see a man hold a door open for an elderly lady, we think he’s being polite; if the woman is young and attractive, we likely attribute a quite different motive.

Liking

Social engineers frequently take advantage of the fact that all of us are more likely to say “yes” to requests from people we like.

Example: Whurley was able to get useful information from Lenore, the girl he met at the fitness center, in part by using “cold reading” to gauge her reactions and continually tailor his remarks to things she would respond to. This led her to feel that they shared similar tastes and interests (“Me, too!”). Her sense of liking him made her more open to sharing the information he wanted to get from her.

People like those who are like us, such as having similar career interests, educational background, and personal hobbies. The social engineer will frequently research his target’s background and equip himself to feign an interest in things the target cares about — sailing or tennis, antique airplanes, collecting old guns, or whatever. Social engineers can also increase liking through the use of compliments and flattery, and physically attractive social engineers can capitalize on their attractiveness to increase liking.

Another tactic is the use of name-dropping of people that the target knows and likes. In this, the attacker is trying to be seen as part of the “in group” within the organization. Hackers also use flattery or compliments to stroke the ego of the victim, or target people within the organization who have recently been rewarded for some accomplishment. Ego stroking may nudge the unsuspecting victim into the role of a helper.

Fear

A social engineer will sometimes make his or her target believe that some terrible thing is about to happen, but that the impending disaster can be averted if the target does as the attacker suggests. In this way, the attacker uses fear as a weapon.

Example: In the story, “The Emergency Patch,” appearing in Chapter 12 of The Art of Deception, the social engineer scares his victim with the threat that the victim will lose valuable data unless the victim agrees to have an emergency “patch” installed on the company’s database server. The fear makes the victim vulnerable to the social engineer’s “solution.”

Status-based attacks frequently rely on fear. A social engineer masquerading as a company executive may target a secretary or junior staffer with an “urgent” demand, and with the implication that the underling will get into trouble, or might even get fired, for not complying.

Reactance

Psychological reactance is the negative reaction we experience when we perceive that our choices or freedoms are being taken away. When in the throes of reactance, we lose our sense of perspective as our desire for the thing we have lost eclipses all else.

Example: Two stories in The Art of Deception illustrate the power of reactance — one based on threats concerning the loss of access to information, the other on the loss of access to computing resources.

In a typical attack based on reactance, the attacker tells his target that access to computer files won’t be available for a time, and names a time period that would be completely unacceptable. “You’re not going to be able to access your files for the next two weeks, but we’ll do everything possible to make sure it won’t be any longer than that.” When the victim becomes emotional, the attacker offers to help restore the files quicker; all that’s needed is the target’s username and password. The target, relieved at a way to avoid the threatened loss, will usually comply gladly.

The other side of the coin involves using the scarcity principle to coerce the target into pursuing a promised gain. In one version, victims are drawn to a Web site where their sign-on information or their credit card information can be stolen. How would you react to an email that promised a brand-new Apple iPod for \$200 to the first 1,000 visitors to a particular Web site? Would you go to the site and register to buy one? And when you register with your email address and choose a password, will you use choose the same password that you use elsewhere?

COUNTERMEASURES

Mitigating social engineering attacks requires a series of coordinated efforts, including the following:

- Developing clear, concise security protocols that are enforced consistently throughout the organization
- Developing security awareness training
- Developing simple rules defining what information is sensitive
- Developing a simple rule that says that whenever a requestor is asking for a restricted action (that is, an action that involves interaction with computer-related equipment where the consequences are not known), the requestor's identity must be verified according to company policy
- Developing a data classification policy
- Training employees on ways to resist social engineering attacks
- Testing your employee's susceptibility to social engineering attacks by conducting a security assessment

The most important aspect of the program calls for establishing appropriate security protocols and then motivating employees to adhere to the protocols. The next section outlines some basic points to consider when designing programs and training to counter the social engineering threat.

Guidelines for Training

Following are some guidelines for training:

- *Raise awareness that social engineers will almost certainly attack their company at some point, perhaps repeatedly.*

There may be a lack of general awareness that social engineers constitute a substantial threat; many are not even aware that the threat exists. People generally don't expect to be manipulated and deceived, so they get caught off guard by a social engineering attack. Many Internet users have received an email purportedly from Nigeria that requests help in moving a substantial amount of money to the States; they offer a percentage of the gross for this kind assistance. Later, you're requested to advance some fees to initiate the transfer process, only to be left holding the bag. One lady in New York recently fell for the scam and "borrowed" hundreds of thousands of dollars from her employer to advance the fees. Rather than spending time on her new yet-to-be-purchased yacht, she is facing the prospect of sharing a bunk bed in a federal detention facility. People really do fall for these social engineering attacks; otherwise, the Nigerian scammers would stop sending the emails.

- *Use role-playing to demonstrate personal vulnerability to social engineering techniques, and to train employees in methods to resist them.*

Most people operate under the illusion of invulnerability, imagining they're too smart to be manipulated, conned, deceived, or influenced. They believe that these things only happen to "stupid" people. Two methods are available to help employees understand their vulnerability and make them true believers. One method involves demonstrating the effectiveness of social engineering by "burning" some employees prior to their participation in a security awareness seminar, and then having them relate their experiences in class. Another approach is to demonstrate vulnerability by analyzing actual social engineering case studies to illustrate how people are susceptible to these attacks. In either case, the training should examine the mechanism of the attack, analyzing why it worked, and then discussing how such attacks can be recognized and resisted.

- *Aim to establish a sense in the trainees that they will feel foolish if manipulated by a social engineering attack after the training.*

Training should emphasize each employee's responsibility to help protect sensitive corporate assets. In addition, it's vital that the designers of the training recognize that the motivation to follow security protocols in certain situations only

grows out of an understanding of why the protocols are necessary. During security-awareness training, the instructors should give examples of how the security protocol protects the business, and the harm that could befall the company if people ignore them or are negligent.

It's also useful to emphasize that a successful social engineering attack may jeopardize the personal information of the employee and his or her friends and associates in the company. A company's human resources database may contain personal information that would be extremely valuable to identity thieves.

But the best motivating factor may be that no one likes to be manipulated, deceived, or conned. As such, people are highly motivated not to feel foolish or stupid by falling for some scam.

Programs for Countering Social Engineering

Following are some basic points to consider when designing programs:

- *Develop procedures for employee actions when a social engineering attack is recognized or suspect.*

The reader is referred to the extensive handbook of security policies provided in *The Art of Deception*. These policies should be considered as a reference; take what you need and leave the rest. Once the company's procedures have been developed and put into use, the information should be posted on the company's intranet, where it is quickly available. Another excellent resource is Charles Cresson Wood's treatise on developing information security policies, *Information Security Policies Made Easy* (San Jose, CA: Baseline Software, 2001).

- *Develop simple guidelines for employees, defining what information the company considers sensitive.*

Since we process information in heuristic mode much of the time, simple security rules can be designed to raise a red flag when requests are made involving sensitive information (such as confidential business information like an individual's password). Once an employee recognizes that sensitive information or some computer action has been requested, he or she can refer to the security policy handbook on the company intranet Web page to determine the correct protocol or procedures to follow.

In addition, it's important to understand and to convey to employees that even information not considered as sensitive may be useful to a social engineer, who can collect nuggets of seemingly useless information that can be joined to provide information for creating the illusion of credibility and trustworthiness. The name of the project manager on a sensitive company project, the physical location of a team of developers, the name of the server that a particular employee uses, and the project name assigned to a secret project are all significant, and each company needs to weigh the needs of the business against the possible threat to security.

These are just a few of the many examples of seemingly unimportant information that can be of use to an attacker. Scenarios such as those in *The Art of Deception* can be useful in conveying this notion to trainees.

- *Modify organization politeness norms — It's okay to say "no"!*

Most of us feel awkward or uncomfortable saying "no" to others. (A product now on the market is designed for people who are too polite to hang up on telemarketers. When a telemarketer calls, the user presses the * key and hangs up; a voice then says to the caller, "Pardon me, this is the Phone Butler and I have been directed to inform you that this household must regretfully decline your inquiry." I love the "regretfully." But I think it an interesting commentary that so many people need to buy an electronic device to say "no" for them. Would *you* pay \$50 for a device that saves you the "embarrassment" of saying "no"?)

The company's social engineering training program should have as one of its goals the redefining of the politeness norm at the company. This new behavior would include politely declining sensitive requests until the identity and authorization of the requestor can be verified. For example, the training might include suggesting responses on the order of, "As employees of Company X, we both know how important it is to follow security protocols. So, we both understand that I'm going to have to verify your identity before complying with your request."

- *Developing procedures to verify identity and authorization.*

Each business must develop a process to verify identity and authorization of people requesting information or actions from employees. The verification process in any situation will

necessarily depend on the sensitivity of the information or action being requested. As with many other issues in the workplace, the security needs must be balanced against the business needs of the organization.

This training needs to address not just the obvious techniques but subtle ones as well, such as the use of a business card by Whurley to establish his credentials. (Recall the title character played by James Garner in the 1970s detective series *The Rockford Files*, who kept a small printing press in his car so he could print up an appropriate business card for any occasion.) We provided a suggestion for the verification procedure in *The Art of Deception*.²

- *Get top management buy-in.*

This is, of course, almost a cliché: Every significant management effort starts with the awareness that the program will need management support to succeed. Perhaps there are few corporate efforts in which this support is more important than security, which daily grows more vital, yet which does little to further corporate revenues and so often takes a back seat.

Yet, that fact only makes it all the more important that a commitment to security start from the top.

On a related note, top management should also send two clear messages on this subject. Employees will *never* be asked by management to circumvent any security protocol. And no employee will get into trouble for following security protocols, even if directed by a manager to violate them.

On a Lighter Note: Meet the Manipulators in Your Own Family — Your Children

Many children (or is it most?) have an amazing degree of manipulative skill — much like the skill used by social engineers — which in most cases they lose as they grow up and become more socialized. Every parent has been the target of a child's attack. When a youngster wants something badly enough, he or she can be relentless to a degree that at the same time is highly annoying, but also funny.

As Bill Simon and I were finishing this book, I was witness to a child's full-bore social engineering attack. My girlfriend Darci and her nine-year-old daughter Briannah had joined me in Dallas while I was there on business. At the hotel on the last day before catching an evening flight,

Briannah tested her mother's patience by demanding they go to a restaurant she had chosen for dinner, and threw a typically childish temper tantrum. Darci applied the mild punishment of temporarily taking away her Gameboy and telling her she could not use her computer games for a day.

Briannah put up with this for a while, then, little by little, began trying different ways of convincing her mother to let her have her games back, and was still at it when I returned and joined them. The child's constant nagging was annoying; then we realized she was trying to social engineer us and started taking notes:

- “I’m bored. Can I please have my games back.” (Spoken as a demand, not as a question.)
- “I’ll drive you crazy unless I can play my games.” (Accompanied by a whine.)
- “I won’t have anything to do on the plane without my games.” (Spoken in a tone of “Any idiot would understand this.”)
- “It would be okay if I played just one game, wouldn’t it!?” (A promise disguised as a question.)
- “I’ll be good if you give me my game back.” (The depths of earnest sincerity.)
- “Last night I was really good so why can’t I play a game now?” (A desperate attempt based on muddled reasoning.)
- “I won’t do it ever again. (Pause.) Can I play a game now?” (“Won’t ever do it again” — how gullible does she think we are?)
- “Can I have back it now, *please?*” (If promises don’t work, maybe a little begging will help . . .)
- “I have to go back to school tomorrow, so I won’t be able to play my game unless I can get started now.” (Okay, how many different forms of social engineering are there? Maybe she should have been a contributor to this book.)
- “I’m sorry and I was wrong. Can I just play for a little while?” (Confession may be good for the soul but may not work very well as manipulation.)
- “Kevin made me do it.” (I thought only hackers said that!)
- “I’m really sad without my game.” (If nothing else works, try looking for a little sympathy.)
- “I’ve gone more than half the day without my game.” (In other words, “How much suffering is enough suffering?”)

- “It doesn’t cost any money to play.” (A desperate attempt to guess at what her mother’s reason could be for extending the punishment so long. Bad guess.)
- “It’s my birthday weekend and I can’t play my games.” (Another pitiful grab for sympathy.)

And continuing as we prepared to head for the airport:

- “I’ll be bored at the airport.” (In the forlorn hope that boredom would be considered a fearsome thing to be avoided at all costs. Maybe if Briannah got bored enough, she might try drawing pictures or reading a book.)
- “It’s a three-hour flight and I’ll have nothing to do!” (Still some hope she might break down and open the book that had been brought along.)
- “It’s too dark to read and it’s too dark to draw. If I play a game, I can see the screen.” (The forlorn attempt at logic.)
- “Can I at least use the Internet?” (There must be *some* compromise in your heart.)
- “You’re the best mom in the world!” (She is also skilled at using compliments and flattery in a feeble attempt to get what she wants.)
- “It’s not fair!!!” (The final, last-ditch effort.)

If you want to increase your understanding of how social engineers manipulate their targets and how they move people from a thinking state into an emotional state . . . just listen to your kids.

THE BOTTOM LINE

In our first book together, Bill Simon and I labeled social engineering as “information security’s weakest link.”

Three years later, what do we find? We find company after company deploying security technologies to protect their computing resources against technical invasion by hackers or hired industrial spies, and maintaining an effective physical security force to protect against unauthorized trespass.

But we also find that little attention is given to counter the threats posed by social engineers. It is essential to educate and train employees about the threat and how to protect themselves from being duped into

assisting the intruders. The challenge to defend against human-based vulnerabilities is substantial. Protecting the organization from being victimized by hackers using social engineering tactics has to be the responsibility of each and *every* employee — *every* employee, even those who don't use computers in performance of their duties. Executives are vulnerable, frontline people are vulnerable, switchboard operators, receptionists, cleaning crew staff, garage attendants, and most especially, new employees — all can be exploited by social engineers as another step toward achieving their illicit goal.

The human element has been proven to be information security's weakest link for ages. The million dollar question is: Are you going to be the weak link that a social engineer is able to exploit in your company?

NOTES

1. The remark by psychologist Neidert can be found online at www1.chapman.edu/comm/comm/faculty/thobbs/com401/socialinfluence/mindfl.html.
2. See Kevin D. Mitnick and William L. Simon, *The Art of Deception* (Wiley Publishing, Inc., 2002), pp. 266–271.

**PSEUDO OPERATIONS AND COUNTERINSURGENCY:
LESSONS FROM OTHER COUNTRIES**

Lawrence E. Cline

June 2005

Visit our website for other free publication downloads

<http://www.carlisle.army.mil/ssi>

[To rate this publication click here.](#)

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, <http://www.carlisle.army.mil/ssi/>, at the Publishing button.

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244.

All Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. Hard copies of this report also may be ordered from our Homepage. SSI's Homepage address is: <http://www.carlisle.army.mil/ssi/>

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please let us know by e-mail at SSI_Newsletter@carlisle.army.mil or by calling (717) 245-3133.

ISBN 1-58487-199-7

FOREWORD

This monograph examines the role of pseudo operations in several foreign counterinsurgency campaigns. Pseudo operations are those in which government forces disguised as guerrillas, normally along with guerrilla defectors, operate as teams to infiltrate insurgent areas. This technique has been used by the security forces of several other countries in their operations, and typically it has been very successful.

A number of factors must be taken into account before attempting pseudo operations, especially their role in the intelligence and operational systems. Although it is likely that most insurgent movements have become more sophisticated, many of the lessons learned from previous pseudo operations suggest their continued usefulness in counterinsurgency campaigns.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

BIOGRAPHICAL SKETCH OF THE AUTHOR

LAWRENCE E. CLINE is a regular instructor with the Center for Civil-Military Relations, Naval Postgraduate School, Monterey, California. He provides programs for foreign military and government officials in developing national counterterrorism strategies and in intelligence reform. He also is a professor of intelligence studies at American Military University and adjunct professor at Troy University and Norwich University. Dr. Cline is a retired U.S. Army Military Intelligence officer, and was trained as a Middle Eastern Foreign Area officer. He served as a United Nations (UN) Military Observer in Egypt and in Lebanon during its civil war; a staff officer with 7th Special Forces Group; advisor in El Salvador during its civil war; senior intelligence analyst with Central Command during Operation DESERT STORM; and as intelligence production chief for United Task Force (UNITAF) in Somalia. His final assignment was as Chief, Middle East Intelligence Branch, J-2, Joint Chiefs of Staff. Dr. Cline earned his Ph.D. in Political Science from the State University of New York at Buffalo, with his dissertation on Islamically-based insurgent movements.

SUMMARY

Pseudo operations, in which government forces and guerrilla defectors portray themselves as insurgent units, have been a very successful technique used in several counterinsurgency campaigns. Pseudo teams have provided critical human intelligence and other support to these operations.

These operations, although of considerable value, also have raised a number of concerns. Their use in offensive missions and psychological operations campaigns has, at times, been counterproductive. In general, their main value has been as human intelligence collectors, particularly for long-term background intelligence or for identifying guerrilla groups that then are assaulted by conventional forces. Care must be taken in running these operations both to avoid going too far in acting like guerrillas, and in resisting becoming involved in human rights abuses.

Just who should control pseudo operations has been somewhat contentious, but the teams typically have worked for police services or intelligence agencies. This has been largely a result of weaknesses in the military intelligence system. Ideally, strengthening military intelligence structures to support pseudo operations would be the best solution since it would provide better connectivity between the pseudo teams and response forces.

Several factors have marked successful pseudo operations. First has been a system of incentives for insurgents to defect to the government. These incentives can be positive, usually monetary rewards for surrendering; or negative, causing insurgents to cooperate to avoid severe punishment. A mix of these forms has proven to be very effective, with very few incidents of insurgents redefecting to the guerrilla side. In general, the role of guerrilla defectors has been critical in successful operations.

A critical environmental factor enabling pseudo team success is weakness in insurgent command and communications systems. Pseudo forces can thrive in environments in which guerrilla forces have problems in their communications and in which centralized control of the guerrilla groups has been weakened. Pseudo teams,

in fact, can help create a synergistic cycle by further weakening insurgent command and control, leading to even more opportunities for their use.

The final critical element of these operations is the effectiveness of the response to the intelligence the teams collect, and coordination with other government forces. Unless government response forces, whether military, police, or intelligence services, are well-trained and prepared to take full advantage of the intelligence provided by pseudo teams, these operations are unlikely to have their maximum impact. Also, unless secure systems are established to avoid interference between the pseudo groups and other security forces, the teams can be in as much danger from their own side as they are from the insurgents.

Pseudo operation strategies used in earlier counterinsurgency campaigns can offer valuable lessons for future missions. It is likely that most guerrilla movements have become more sophisticated in their operations; as a result, pseudo teams must also develop better techniques. Still, the pseudo operations strategy should provide major benefits against insurgent groups.

PSEUDO OPERATIONS AND COUNTERINSURGENCY: LESSONS FROM OTHER COUNTRIES

The term “pseudo operations” (or some variant of it) indicates the use of organized teams which are disguised as guerrilla groups for long- or short-term penetration of insurgent-controlled areas. They should be distinguished from the more common police or intelligence infiltration of guerrilla or criminal organizations. In the latter case, infiltration is normally done by individuals. Pseudo teams, on the other hand, are formed as needed from organized units, usually military or paramilitary.

The use of pseudo teams has been a hallmark of a number of foreign counterinsurgency campaigns. In most cases, these operations have been very successful. This monograph examines the record of several of these cases, discusses some issues raised by these types of operations, and suggests key lessons learned.

THE HUK INSURRECTION

An early example of pseudo-guerrillas was during the Huk Insurrection in the Philippines from 1946-55. The principal unit to be devoted to pseudo operations was the so-called Force X. The group initially was formed in 1948 by members of the Philippine Constabulary:

The basic idea was to make this specially trained force into a realistic pseudo-Huk unit that could, in enemy guise, infiltrate deep into enemy territory. The 47 initial members of Force X were dressed and equipped like Huks. They were taught in a remote rain forest base to talk and act like Huks by four captured guerrillas who had been “tested, screened, and reindoctrinated to our side and brought to the training base to serve as instructors.” The principal aim was to enable government forces to get close enough to guerrilla forces to eliminate selected targets.¹

One very successful mission of this type is worth describing for an indication of how the Force X concept was used:

Accompanied by three military intelligence agents, a group of 20 former Huks were infiltrated into [Panay’s] interior. After 3 months of gathering

information, establishing their cover as a bona fide Huk unit, and gaining the confidence of the island's Huk leadership, they hosted a "by invitation only" barbecue for the Panay High Command. Between the ribs and potato salad, the covert government force sprang an ambush that killed or captured nearly all the Panay commanders and crippled the organization on the island for the duration of the campaign.²

Beyond the assassination campaign against the Huk cadre, the members of Force X also engaged in psychological operations and various "dirty tricks" campaigns, to include planting doctored ammunition in Huk ammunition caches that would explode when fired.³ They also were used for long-term intelligence collection.

A similar unit to Force X was established later in the anti-Huk campaign. This was called Charlie Company. Due to the Huks' awareness of earlier Force X operations, Charlie Company operations normally did not involve actually trying to link with guerrilla groups. Instead, they operated small team reconnaissance operations while dressed either in uniform or in guerrilla disguises; in some cases, they would also conduct "snatch" missions while dressed as guerrillas.⁴

MALAYA

During the same period, the British were conducting generally similar pseudo operations in their campaign against the Malayan Races Liberation Army (MRLA), a predominantly Chinese-based insurgent group. This group was called "communist terrorists" (CTs) by the British. Originally, the use of pseudo-guerrillas was bottom driven, with police Special Branch officers in the districts initiating the teams.

One of these operations typified the use of pseudo teams. A Special Branch officer established links with a MRLA section leader by arranging for his wife to deliver her baby in a government hospital. After becoming closer to the leader, the Special Branch officer made a deal with him. The leader led a column of six insurgents out of the jungle into a deliberate ambush in which the leader was carefully identified ahead of time and spared. Chinese British soldiers then donned the dead insurgents' uniforms and were led back into the jungle by the MRLA member. From there, they operated against higher ranking members of the insurgency.⁵

Robert Thompson, one of the principal civilian architects of the counterinsurgency campaign argued that the captured insurgents,

needed to “belong” to some organization in place of the Communism they had renounced; he believed they tended to turn to other ex-CTs for guidance in the new world into which they had just emerged . . . [I]n a strange way they could only justify their escape from Communism by being personally involved in the struggle against it—which was why time after time they begged to lead patrols back into the jungle to attack their former comrades.⁶

Another author offered a more practical reason for the willingness of captured or surrendered insurgents to cooperate: They needed “to kill off all the Communists who knew them, and knew of their defection or capture, before this news could be spread around to the Traitor Killing Squads, which might extract retribution from relatives.”⁷ Whether from practical considerations or more complicated psychological factors, surrendered or captured MRLA members tended to cooperate with British authorities once under their control.

In Malaya, one aspect of dealing with surrendered or captured guerrillas presented a difficulty that has surfaced in other campaigns. Psychological operations campaigns stressed the good treatment of surrendered insurgents in an effort to inspire others to surrender voluntarily. For other guerrillas to believe this approach, however, it was necessary to publicize the current satisfaction of those who had already surrendered through photographs and broadcasts.⁸ This approach, of course, conflicted with the requirement to keep hidden the identities of those guerrillas who had agreed to cooperate as pseudo-guerrillas.

The British also used pseudo-guerrillas for some psychological operations including disguising some troops as MRLA members, then launching a false bombing raid on their position. The troops were made up to look wounded and then sent into areas where they would encounter insurgents and spread tales of the effectiveness of British targeting. In general, however, the pseudo teams were used for intelligence collection and to target guerrilla camps for bombing raids.

KENYA AND THE MAU MAU

From 1952 to 1960, the British fought a counterinsurgency campaign against the tribally-based insurgent group called the Mau Mau in Kenya. The command and control system for British operations in Kenya consisted of provincial headquarters, with a provincial emergency committee consisting of police and army representatives, and district committees established below them with similar members.

The group with the principal responsibility for intelligence collection was the Special Branch of the police rather than military intelligence officers. Due to the increased demands placed on Special Branch by the Mau Mau operations, the army seconded sergeants from the Kenya Regiment to serve as Field Intelligence Assistants (FIAs). These FIAs were posted to "outlying parts" of the districts to collect information.⁹

After the FIA system was established, the army headquarters then began assigning some army officers at the district level as District Military Intelligence Officers (DMIO) to work with the Special Branch officers. It was not until later in the counterinsurgency campaign that an army officer was assigned to Special Branch headquarters to serve as the principal liaison to coordinate the operations of the army and Special Branch nationally.¹⁰

Most of the officers and noncommissioned officers had little or no formal intelligence training or background. Frank Kitson, who was key in developing the concept of pseudo-guerrillas in Kenya, noted the attitude of his superiors when he was appointed as a DMIO: "[I]f we could not be of any use, could we please not be a nuisance?"¹¹

Kitson's original concept was simply to develop camps in which the British "could keep a handful of Africans who could help [the FIA] with his interrogations and who could move around the countryside planting . . . and visiting informers."¹² In rather short order, however, he discovered that captured Mau Mau were willing to work actively against their former comrades. Former Mau Mau were used to train British African troops and deployed with these troops in the field against the insurgents. As with Malaya, the initial deployment of the pseudo-guerrillas was bottom driven, with official approval from

the British headquarters following only after a number of operations had been run. In about a year, the original small pseudo group had grown to a force of about 200.¹³

These teams were used primarily to collect long-term information and intelligence since, as Kitson notes, “. . . if we always directed Security Forces onto gangs immediately after visiting them, the terrorists would soon tumble to the idea.”¹⁴ It was only when a particularly valuable target was encountered that the teams would launch direct attacks, unless, of course, a team came under immediate threat. Even when the pseudo teams (normally called “pseudo gangs” by the British) launched direct operations against insurgent groups, they typically tried to capture as many as possible rather than to kill them.

One tool that proved very useful in identifying Mau Mau members—a number of whom then were turned to the government’s side—was the “hooded man” system:

The Coleman Scheme was to have many more hooded men than Special Branch had used. He wanted at least 10 each time and possibly more . . . The FIA would then disguise the man before he came into contact with the other hooded men, some of whom might be prisoners rather than informers. When they were all safely hidden behind their masks, they would be assembled and sat down in a row of chairs, with one of our men standing behind each one. No hooded man was allowed to talk to another . . . When all was ready, the suspects would walk past the hooded men. If they recognized anyone they would give brief particulars to the FIA standing behind their chair. If a suspect was recognized by three or four of the hooded men and if the particulars given to the FIAs corresponded, then it was a safe assumption that they had picked the right man. In this way, we collected a lot of information about people, and we also caught many senior Mau Mau supporters. Quite often we would even get active gangsters in the net.¹⁵

Although Kitson admitted that it was a “gross oversimplification,” he noted that in terms of recruiting former insurgents to serve with the pseudo teams, the Mau Mau could be divided into three categories. The first was what might be termed the “true believers,” for whom “the only thing to do was to give him away as soon as possible.” The second category was those who “had merely joined because all their friends had done so, and because life was getting rough in the

Reserve." In general, Kitson found them unsuitable for the teams. The final category was "the Africans who joined the gangs from a spirit of adventure." He found the last group to be the best prospects for his teams.¹⁶

Training—or "taming" as Kitson calls it—of guerrilla defectors for the pseudo teams involved three phases. The first phase involved harsh treatment of the prisoner, including chaining him and feeding him only the most basic food. In the second stage, "the candidate would be incorporated gradually into the community as a friend but would not be told much about the business nor would he be left by himself." Finally, "[h]e could sleep with the others, carry arms, do sentry duty or go out by himself." Kitson states that after the system became fully implemented, the whole process could occasionally be completed in as little as 24 hours.¹⁷

Early operations of the pseudo gangs took place primarily in settled areas rather than in the "forest." As the Mau Mau began being forced away from the population, the pseudo team concept expanded to longer-term jungle operations, which put much more stress on the teams.¹⁸ They did have some success in their operations, although it does not appear to have resulted in as much impact as in their previous operations.

Although most of the pseudo gangs' activities involved very small scale operations, they had a definite impact on the counterinsurgency campaign. Kitson concluded that by 1954 his teams "had probably accounted for more actual gang members and weapons than any of the large military operations in the past six months."¹⁹ Since the guerrillas operated predominantly in small groups, with problems in communications between the various groups, the environment was ideal for pseudo operations.

THE FRENCH EXPERIENCE

The French military in Indochina and Algeria would have seemed well-placed to use pseudo operations extensively. During the French campaign in Indochina, about 325,000 of the 500,000 French troops were Indochinese, giving them a natural base for pseudo forces.²⁰ Nevertheless, virtually all these native troops were used in conventional units.

The French, however, did establish guerrilla groups based on native tribal groups. These units, called the *Groupeement de Commandos Mixtes Aéroportés* (Composite Airborne Commando Group or GCMA)—later renamed the *Groupeement Mixte d'Intervention* (GMI) or Mixed Intervention Group—were intended to conduct guerrilla operations to attack Viet Minh rear areas. The GCMA was a subordinate element of the *Service de Documentation Extérieure et de Contre-Espionnage* (French Counterintelligence Service) in Indochina. Although relatively effective, the GCMA basically was a “conventional” guerrilla force rather than a form of pseudo operation.²¹

In Algeria, the French used a large number of native Algerian troops called *harkis*. In total, over 180,000 *harkis* served in the war, a larger number of troops than was fielded by the FLN (National Liberation Front, the independence group).²² These soldiers generally were used in conventional formations either in all-Algerian units commanded by French officers or in mixed units. They also were employed as platoon or below sized units attached to French battalions in a role akin to the use of Kit Carson Scouts by the United States in Vietnam.²³ *Harki* units in this third use were designed primarily in an intelligence gathering role, with some reported minor pseudo operations in support of their intelligence collection.²⁴ The extent of these pseudo operations appears to have been very limited both in time and scope, however.

The most widespread use of pseudo type operations was during the “Battle of Algiers” in 1957. The principal French employer of covert agents in Algiers was the Fifth Bureau, the psychological warfare branch. In addition to other better known French counterinsurgency measures such as a block warden system and widespread use of torture to extract information, the Fifth Bureau also made extensive use of “turned” FLN members:

Among the most specialised stratagems within intelligence-led counter terrorism was the ploy to reverse the loyalties of captured FLN militants, so that after being interrogated they worked for French intelligence . . . [Captain Paul-Alain] Leger [of the 10th Paras] ran a network of former FLN activists whom he “turned” and sent back into the Algiers Casbah after “persuading” them to change sides by torture or by threats against their families. These agents were disguised as street sweepers and

municipal workers . . . [and] mingled with the FLN cadres. They planted incriminating forged documents, spread false rumours of treachery and fomented distrust among the [FLN] . . . As a frenzy of throat-cutting and disemboweling broke out among confused and suspicious FLN cadres, nationalist slaughtered nationalist from April to September 1957 and did France's work for her.²⁵

It should be noted that this form of pseudo operation apparently involved individual operatives rather than organized units as discussed in other cases. Using individuals rather than teams in this case may, in fact, have been a more appropriate response since the FLN inside Algeria by this point was very fragmented in terms of operational control.²⁶

As with the case of Indochina, rather than trying large-scale pseudo-guerrilla operations, the French focused on developing native guerrilla groups that would fight against the FLN. They had some success with a group in the Southern Atlas Mountains, providing it with arms and supplies.²⁷ Unfortunately for the French, they also had a disaster with another group called "Force K."

In this case, the FLN essentially used pseudo-guerrilla strategies against the French guerrilla group. Some 1,000 Algerians volunteered to serve in Force K as guerrillas for the French. Most of the members of Force K either were FLN members already or were turned by the FLN once enlisted. Although Force K's operations initially looked promising, complete with the corpses of purported FLN members displayed by the unit, these bodies were in actuality those of dissidents and members of other Algerian groups killed by the FLN. Eventually, upon discovery by the French of the sympathies of the majority of "its" guerrillas, the French army tried to hunt down and kill its members. Despite French efforts, however, some 600 managed to escape and join the FLN with their weapons and equipment.²⁸

RHODESIA AND THE SELOUS SCOUTS

The Rhodesian insurgency developed gradually, initially appearing to be more of a law enforcement problem than an organized insurgency. It took considerable time for the Rhodesian government to acknowledge the severity of the insurgent threat it faced and to

develop a coherent response.²⁹ Ultimately, the government faced two different major insurgent groups: the Zimbabwe African People's Union (ZAPU), together with its military arm, the Zimbabwe People's Revolutionary Army (ZIPRA); and the Zimbabwe African National Union (ZANU), with its military wing, the Zimbabwe National Liberation Army (ZANLA). These two groups, largely tribal based, used two very different strategies—ZIPRA focused on conventional Soviet-style operations, while ZANLA operated under a Maoist rural strategy. Neither group cooperated with the other; in fact, there were clashes between the two.

Intelligence operations in Rhodesia—together with overall coordination of counterinsurgency—remained very complicated. There were a series of joint operations centers at various levels that combined the police and the military; in practical terms, however, the army almost always had the major authority. The senior planning level was at the Operations Coordination Committee, which combined the commanders of the army and air force, the Commissioner of Police, and the Director of the Central Intelligence Organization. As one study noted, "all decisions had to be reached through an arduous system of consensus, with each member retaining the responsibility for ensuring that his service carried out agreed-upon command decisions."³⁰

By 1977, in an effort to improve centralized planning, the post of Commander, Combined Operations (COMOPS) was created. The Rhodesian security system, however, never did have a completely unified headquarters, and overall planning remained somewhat shaky.³¹ This was particularly true for Special Forces, including the Selous Scouts. With the formation of COMOPS, all Special Forces units were removed from army control. Instead, they were controlled directly by COMOPS Commander Lieutenant General Peter Walls. The only role the army headquarters played was to provide administrative and logistics support. Also, there was no central Special Forces headquarters, and no Special Forces-qualified officers were assigned to COMOPS.

A particular gap in Rhodesia's counterinsurgency campaign was that of intelligence. Virtually all the effective intelligence being provided was through the police Special Branch. The military

intelligence system was very weak throughout the war. In most cases, units below brigade level had only a corporal for their intelligence officer. At all levels, the job of intelligence officer was "... to be filled by someone not suitable for any other post. It was also considered the first ready-use pool of officers and other ranks, should a shortage of personnel occur elsewhere."³²

Even after the formation of COMOPS, the intelligence system remained very weak:

... [L]ack of a central body for coordinating intelligence at COMOPS also had a decidedly negative effect on the total intelligence effort. Initially the section consisted of a single member ... This neglect had also led to an almost total lack on military intelligence officers capable of control and co-ordination of intelligence at top level and to the neglect of military intelligence as a serious challenge at lower level.³³

The original impetus for pseudo operations came from regional joint operations centers rather than intelligence or police headquarters.³⁴ The main driving force was due to the intelligence problems already discussed: Field units simply were not receiving the intelligence they required to respond to the insurgents. Police made an early attempt to use pseudo operations in October 1966, but the effort was stillborn.³⁵ The first formal pseudo team was formed in January 1973 as an all-African team, with two African policemen and four "turned" insurgents. The early teams did succeed in bringing in some valuable intelligence, but their overall impact was slight.

In November 1973, Major (later Lieutenant Colonel) R. H. Reid-Daly was tasked with forming the Selous Scouts as a pseudo-guerrilla force. Its original membership came largely from army trackers, and its cover throughout most of its existence was as a tracking unit. The original strength of Selous Scouts was about 120, with all officers being white and with the highest rank initially available for Africans being colour sergeant.³⁶ One major recruiting incentive for African volunteers was that their pay was nearly doubled from their normal army salaries due to special bonuses.³⁷ Additionally, somewhere around 800 turned insurgents eventually were recruited, whose salaries were paid by Special Branch.³⁸ Ultimately, the unit reached a strength of somewhere around 1,500.

The original focus of the Selous Scouts was on intelligence gathering for operational forces rather than acting as some form of hunter-killer team: “. . . [O]ur pseudo insurgent groups should only resort to killing insurgents if they had been compromised, or the prize was so extraordinarily great that it was worth the high cost of a compromise.”³⁹ Virtually all the intelligence collected by the pseudo teams was passed to Special Branch, and the “flow of intelligence from the Selous Scouts to local Army commanders was very limited.”⁴⁰

Beyond the internal intelligence operations of the Selous Scouts, they also began conducting an increasing number of external operations. These operations involved both intelligence collection and direct action missions. Much of the impetus for these external operations came from the Selous Scouts themselves, whose leaders continued to push more and more for these types of missions. Reid-Daly argued that:

External operations, although rarely more dangerous than our internal operations, always excited interest and enthusiasm in the troops and proved to be a great morale-booster. They also provided a welcome break from the general tedium, which often bugged our internal pseudo operators.⁴¹

He also notes that the majority of insurgent casualties caused by the Selous Scouts, in fact, were created by external operations.⁴²

A number of the external missions were long-range reconnaissance and surveillance missions, but increasingly included offensive operations. Selous Scouts originally were involved in an assassination attempt against ZIPRA leader Joshua Nkomo in Zambia. This mission, which had to be aborted by the Selous Scouts, later was attempted by the Rhodesian Special Air Service (SAS); the SAS operation was a failure. The Scouts conducted regular operations in Mozambique, Zambia, and Botswana.

In many of these missions, the Selous Scouts would disguise themselves and their vehicles as being part of the neighboring country's forces. Other than this, however, some operations resembled much more conventional raids than they did covert operations. The Rhodesian government normally demanded some

element of “plausible deniability” for these operations—principally by restricting most direct support air missions—but this political fig leaf was very minimal. This became increasingly pronounced as the Selous Scouts conducted larger and larger operations, many involving large motorized columns launched across Rhodesian borders.

Most of these missions were very successful militarily, but their overall political impact was counterproductive. Although the Rhodesians generally tried to avoid inflicting significant numbers of casualties on the soldiers of the countries they entered, such casualties were almost inevitable. Worse, a few operations resulted in the deaths of local civilians.⁴³ Even where the Selous Scouts raids succeeded in striking guerrilla sanctuaries, the political results could be harmful.⁴⁴

A good example of this problem was the Selous Scouts’ raid on a ZANLA camp at Nyadzonya Pungwe, Mozambique in August 1976. Eighty-four Scouts using Rhodesian trucks and armored cars painted in Mozambique military camouflage drove directly into the camp. Once there, they killed some 1,000 purported guerrillas. Militarily, it was a remarkable feat. Unfortunately, the camp was formally registered with the United Nations (UN) as a refugee camp. Also, even by Reid-Daly’s account, most of those killed were unarmed guerrillas standing in formation for a parade.⁴⁵ To make matters worse, the camp hospital was set afire by the rounds fired by the Scouts, burning alive all the patients. The international condemnation of this raid almost certainly outweighed its military success in the long term.⁴⁶

Captured guerrillas were critical in the intelligence operations of the Scouts. The first step in potential recruitment of former guerrillas was in the interrogation process:

For a prisoner to be of any use to us, it was absolutely vital that his identity was totally protected and that neither the locals in the area of the contact, nor anyone back at the security force base, knew of his capture or even of his existence. . . . When a captured insurgent was brought into a Selous Scouts fort, the first priority was to give him the best possible medical attention available . . . [T]he only things said to him were concerned purely with his health and physical welfare. The captive was usually astonished to see that everything had been done to ensure his life

was saved. And because of this, whether consciously or unconsciously, a feeling of gratitude would begin to permeate his mind.⁴⁷

From this point, “in nine cases out of ten, the information just poured out.”

At times, of course, the captured guerrilla’s usefulness was expended after the interrogation. In virtually all cases, however, attempts were made to recruit the prisoners for the Selous Scouts. The group had an excellent track record in its recruiting efforts. It developed a specific routine for “turning” the guerrillas:

. . . [T]he best recruiting method was to send another former insurgent to visit him in hospital . . . and have a long conversation, dwelling in particular upon the hardships the insurgents were experiencing in the bush . . . The process of turning insurgents was eased considerably by the knowledge that they could be hanged as violators of the Law and Order Maintenance Act. He would then be examined thoroughly by members of the Selous Scouts to ensure his loyalty—not to the government of Rhodesia, but to the members of the unit itself. The insurgent also would be offered a cash lump sum for joining the Selous Scouts (together with receiving the same salary as a soldier, with the funds being paid by Special Branch), and if possible, his family would be moved to the Selous Scouts base, where they received free rations, housing, education, and medical care.⁴⁸

The Selous Scouts were the most important element in providing actionable intelligence for the security forces, however questionable the ultimate effects of their external offensive operations. According to a 1978 study by the Directorate of Military Intelligence, 68 percent of all insurgent deaths inside Rhodesia could be attributed to the Selous Scouts.⁴⁹ With this record, the Scouts emerged as the most potent factor in Rhodesia’s counterinsurgency campaign.

OTHER PSEUDO OPERATIONS

Kenya and Rhodesia are the two best known examples of the use of pseudo-guerrillas, but similar techniques have been used in a number of other counterinsurgencies. The Portuguese in particular used pseudo operations extensively in their African colonies in the 1960s and 1970s.

Portuguese pseudo units included the *Tropas Especiais* (Special Troops), *Grupos Especiais* (Special Groups), and *Flechas* (Arrows). At their maximum strength, some 11,000 personnel served in these units, mostly organized in small bands.⁵⁰ These units, consisting both of African troops and “turned” guerrillas, generally were intended for intelligence gathering and were controlled by the Portuguese intelligence service, the International Police for the Defence of the State (PIDE).

Guerrilla recruitment was similar to that in Rhodesia, with positive reinforcement being stressed. In Mozambique, the Portuguese commander “claimed a 90 percent success rate in persuading captured guerrillas to turn against their former colleagues . . .”⁵¹ In Guinea, General Antonio de Spínola reportedly evacuated wounded guerrillas to hospitals before his own troops.⁵²

More recently, the Salvadorans used pseudo teams for intelligence collection during their civil war. The Turkish government also has used Special Teams (sometimes called Special Action Teams) in operations against the Kurdish Partiya Karkeren Kurdistan (PKK). These teams are composed primarily of former army and Jandarma (paramilitary) officers and noncommissioned officers. They normally dress in civilian clothing or PKK uniforms, or as close as the PKK comes to having uniforms. Apparently, the Special Teams do not employ former PKK members as part of the teams. Two particular issues with the Special Teams emerged during the course of their operations. First, they have been accused of “vigilante justice” in executing suspected PKK members. Second, team members reportedly have been recruited heavily from the right-wing Nationalist Action Party.⁵³

ISSUES RAISED BY PSEUDO-GUERRILLAS

The governments that have used pseudo operations clearly have viewed them as very valuable. At the same time, however, the operations that have been conducted have raised a number of problems and issues. Not all these issues are amenable to easy solutions, but should be considered when planning such operations.

Intelligence or Operations?

The two major models of pseudo operations are as intelligence collectors or as operators for direct action missions. In some cases, of course, teams have been used for both roles. The main issue for governments is to determine in which role pseudo teams are most useful?

The main argument for using pseudo teams as intelligence collectors is that by virtue of their training and employment, they are ideally situated for collecting human intelligence. Their ability to blend with actual guerrillas—at least for reasonable periods of time—means that they can collect critical intelligence that likely would be impossible through normal intelligence means.

There are several practical issues involved with using pseudo-guerrillas exclusively for intelligence collection, however. The first is the potential difficulty of extracting these teams before government forces act on their intelligence. Second, the longer teams remain in an area collecting information, the more chance of being unmasked. Finally, there will almost always be a time gap between the time a team collects the intelligence and the time other forces can respond, potentially giving the guerrillas time to escape.

One larger point may militate against using pseudo teams for routine direct offensive missions. This is the potential political impact of such operations. It is all too easy for government opponents to brand the teams conducting these missions as “death squads” beyond the reach of the law. This certainly has been an issue with the Turkish Special Teams. Any mistakes in targeting in which civilians or even unarmed members of a guerrilla support structure are killed can have severe repercussions for the government. This, of course, is even further exacerbated if such operations are cross-border operations, leading to the potential for third country nationals being killed.

Given the potential political problems with direct missions, intelligence collection appears to be the preferable mission for pseudo teams. This, of course, is not completely an either-or proposition. The teams in Kenya likely struck the right balance: When operating independently, their primary goal was always to take prisoners

rather than to inflict casualties. Their attitude was that the potential risks involved in taking prisoners rather than killing the insurgents immediately were very much worth it in terms of the intelligence payoffs.

How Far to Go?

A key issue involving the use of pseudo insurgents is how far they are allowed to go in acting like insurgents. Clearly, unless the teams are accepted as authentic in a process that Cilliers calls “validation,” they will not be productive (and, of course, can be killed). On the other hand, their actions in gaining acceptance typically involve questionable activities.

At times, in fact, their operations have been counterproductive to ultimate government goals. Reid-Daly notes one particular egregious case in which a pseudo group conducted a bogus attack on a protected village. Their initiative so shamed the real ZANLA groups in the area that they started a regular mortaring campaign against the village.⁵⁴ Kitson notes that at times his team members posing as guerrilla leaders ordered the beating and fining of Mau Maus; in fairness, however, these normally were for offenses involving the death penalty under the Mau Mau code.⁵⁵

The very presence of pseudo teams can potentially destabilize an area. As these teams enter an area, they must sell themselves as legitimate guerrillas. Frequently this means conducting propaganda operations with the local populace. Even without active propaganda, the presence of “guerrillas” may well create doubts among locals as to the government’s ability to control its territory and to protect them.

This is an issue for which there are no pat answers. Governments should carefully consider the areas in which they insert pseudo teams and what types of missions the teams are given. Procedures and general rules of engagement should be worked out in advance by the headquarters and team commanders. Beyond this, the key element will remain the training and judgment of the independent teams.

Who Should Control Pseudo Operations?

Virtually all the pseudo teams operated to date have been controlled by either police services—usually in the form of Special Branch or its equivalent—or intelligence agencies. In the cases of Kenya and Malaya, this largely was a function of overall British counterinsurgency doctrine that emphasized the primacy of civilian control.⁵⁶ Rhodesia appears to have followed the British model largely due to its colonial roots from Britain. Other countries such as Portugal, however, also have used a similar structure.

It is logical to put intelligence agencies or the police equivalent of Special Branch in charge of pseudo operations. Both police and intelligence services have experience in conducting undercover or covert activities. As such, they have gained proficiency in such critical issues as maintaining the security of the members involved, establishing covert systems of communications, and in general “tradecraft.”

The principal counterargument, that the teams should be run by the military, is that most police or intelligence undercover operations use individuals rather than formalized teams. Militaries are much more accustomed to handling units than are police or intelligence services. Also, members of pseudo groups normally will require at least basic military tactical skills, for survival, if nothing else. The pseudo units who become involved in offensive operations also are more likely to need military channels to provide support.

Beyond the tactical level, in many cases pseudo teams have grown in overall strength beyond the abilities of police services to directly supervise them. With the Selous Scouts for an example, their growth to about 1,500 strong and a shift to offensive operations would have overwhelmed the capabilities of any police service for direct supervision.⁵⁷ Even with the smaller number of teams in Kenya and after their successes, there was a significant debate within the British administration over whether the pseudo teams should be controlled by Intelligence Branch or the Operations Branch.⁵⁸

Perhaps the key factor in the historical cases leading to police or intelligence control of pseudo operations simply was that the military intelligence systems were so weak. If pseudo teams are to

be used primarily for intelligence operations, then their supporting intelligence system must be capable of rapidly processing the information they collect. If the military intelligence structure is not prepared for adequate support of the human intelligence the teams provide, then some other agency must assume this role.

The ideal solution would be for militaries engaged in counterinsurgency to strengthen their military intelligence system to support pseudo operations if required. This would include augmenting human intelligence coordination and analysis, training in how pseudo operations might be conducted, and establishing at least the framework for supporting teams. This likely would be particularly important if governments use military units as response forces to the intelligence provided by pseudo teams. Using military intelligence as the link between the teams and military response forces provides more streamlined bureaucratic channels for processing immediate intelligence.

What Type of Intelligence Should Pseudo Teams Provide?

There are several issues surrounding the intelligence provided by pseudo teams. The first is how to handle insurgents who have been captured as a result of team operations. A particular question is that of what should be gained from interrogations since this is typically the first stage of recruitment.

There are two opposing views as to the issues surrounding the use of interrogation of captured insurgents. Frank Kitson notes that if immediate tactical information is needed, direct interrogation is required. This must be accomplished by local commanders, who require detailed intelligence for their tactical operations. On the other hand, background intelligence for long-term operations is best achieved by Special Branch. Acquiring this form of intelligence requires a very different approach: "[T]he chief use of a prisoner lies in gaining his co-operation and friendship, and a different process, which takes much longer, is required."⁵⁹

Reid-Daly, on the other hand, stressed the absolute criticality of focusing on immediate tactical intelligence:

Insurgent prisoners, immediately after capture, provided the best, immediate and hottest up-to-the-minute intelligence. But the speed of the acquisition of such intelligence was governed by the time it took to make the prisoner talk . . . It was important, therefore, that a captive was speedily broken, and the intelligence gained from him quickly acted upon. If this did not happen, the security forces gained nothing.⁶⁰

The same competing approaches can be applied to pseudo operations more generally. Pseudo teams can provide a key contribution to the current intelligence picture. The problem of acquiring immediate intelligence was described well by Reid-Daly:

It is of little use to a soldier to know where the insurgents were yesterday, or even where they might be tomorrow. He needs to know where they are **now**, so that he can do something about it. And this, in effect, was the fundamental problem—the acquisition of intelligence, which could be immediately acted upon.⁶¹

The opposite approach taken by Kitson is to focus pseudo operations on developing long-term intelligence rather than immediate tactical intelligence. In this approach, short-term intelligence takes a back seat to trying to determine the broader pattern of insurgent operations. If done well, this can be critical in predicting future guerrilla activities and preempting them. Ultimately, this may be of greater benefit in the counterinsurgency campaign.

A second key aspect of using the intelligence collected by pseudo teams is how to use this information. The risk of compromise of operations can be exacerbated by too obvious immediate use of the intelligence provided by a team. If a pseudo team's intelligence reporting of a particular insurgent network results in an immediate "roll up" of the network, it likely will be apparent to the other side what has happened.⁶² This is particularly the case, of course, if such responses occur repeatedly.

This difficulty is a good argument for Kitson's approach. Certainly, some high value targets such as key leaders are worth the risk of exposing the pseudo teams' operations, but in most cases they likely are better used for longer-term collection. As with many other aspects of pseudo operations, governmental responses to their collection activities must be carefully coordinated so that they can continue

to operate without being exposed. One technique successfully used by many teams was to purportedly move out of an area well before government forces arrived, but to maintain covert surveillance of the guerrilla forces they had mixed with.

Should Teams be Used to Conduct Psychological Operations?

In Rhodesia, teams would deliberately violate local customs to alienate the people from the guerrillas. They would also target members of ZANLA and ZAPRA, pretending to be members of the other group. Ultimately, this led to some firefights between the two groups. Likewise, the Philippine government used similar tactics.

Such operations certainly have had some success. Overall, however, they likely are not the best use of pseudo teams. Use of “dirty tricks” can create significant problems for governments when they are discovered. Also, these techniques can create a dangerous situation for civilians, either directly or as a result of guerrilla reprisals. There also is the problem of determining where to draw the line; as these operations develop, the risk of being “overly creative” in new tricks to try is very real.

Are “Outsiders” Essential?

The insistence of both the British in Kenya and the Rhodesians in using white officers led to practical difficulties. Reid-Daly notes the problems in “blackening-up.”⁶³ In most cases involving contacts with the insurgents, the white officers had to hide outside of the village or camp in which their African team members were meeting the guerrillas. In at least one case, however, a team used a white member as a “prisoner” to gain access to a group of guerrillas.⁶⁴

Likewise, in Kenya, the presence of white members always presented security problems. Nevertheless, the mixed race teams typically faced only limited difficulties in “selling” themselves as Mau Mau despite using relatively primitive disguises.⁶⁵ In fact, in one case in which a team unexpectedly encountered a group of Mau Maus, they successfully explained away the white team member with them as being an “Asian Mau Mau.”⁶⁶

Clearly, most, if not all, of the insistence on using white leaders for the teams in Kenya and Rhodesia was a result of colonial heritage and/or racism. In fairness, though, the mixed-race teams seemed to bond very closely, and all the members were treated well.⁶⁷ Also, the guerrillas in both countries seemed to see what they expected to see. In retrospect, the teams got away with what seems in many cases to have been remarkably sloppy tradecraft.

Nevertheless, despite their successes in melding the teams, there seems to be no practical necessity for using such mixed teams. Other countries certainly have succeeded in using pseudo teams that could blend with the guerrillas. Portugal, in fact, started with white-officered units, but rather quickly shifted into all-African teams.⁶⁸ The issue of using “outsiders” is almost certainly even more dangerous, given that most insurgent groups likely have become more sophisticated. There seems to be little practical advantage to using mixed teams.

LESSONS LEARNED

1. Money Counts. In most cases of successful use of pseudo operations, money in one form or another has been a key component of the campaign. Cash rewards both for civilians to turn in insurgents and for insurgents to surrender have provided the basis for the respective governments to seize the guerrillas. This, of course, is the first step in being able to “turn” them. Rewards for turning in guerrillas—usually “dead or alive”—were used in Malaya, the Philippines, Kenya, and Rhodesia.

In a number of cases, reward money was sufficiently ample that guerrilla leaders would turn in their own troops. This became common enough in Malaya that some government officials began expressing concerns as to the amount of money actually being paid out to the insurgent leaders.⁶⁹ In some cases, both cash rewards and relocation were offered to surrendered guerrillas.⁷⁰

Besides cash, in the counterinsurgency campaign against the Huks, the provision of land to a number of the insurgents who turned reportedly was a very successful tactic. The impact of this program was more psychological than practical: “As a resettlement program, The Economic Development Corps (EDCOR) did not

accomplish a great deal. I doubt if more than perhaps 300 families of Huks were resettled under that program. But I will guarantee you that at least 3,000 Huks surrendered. . .”⁷¹ The program became even more restrictive later, limited to only those Huks who actually participated in operations against their former comrades.

In the larger picture, of course, the use of reward money or other inducements as tools for counterinsurgency must be done with some discretion. Originally in Kenya, the British administration offered a bounty of five pounds for the first small units that killed an insurgent.⁷² The result was that few live insurgents were surrendered. Similarly, the use of “wanted dead or alive” bounties is not desirable (except perhaps for major insurgent leaders) since the odds are good that the guerrilla will be brought in dead. First, it must be determined if the person was, in fact, a guerrilla and not simply a personal enemy of the person seeking a reward. Second, a corpse is of little intelligence value.

Where the bounty system has worked very well is when it has been used for getting live guerrillas under government control. This particularly has been an advantage for pseudo operations. It is a relatively small step for an insurgent who has turned himself in to receive a reward and then to agree to actively work for the government for even more money.

2. The alternative to cooperation can be dire. A pattern among the successful efforts at pseudo team recruitment of former guerrillas is that, although the carrot of financial rewards is valuable, the stick of noncooperation can be even more significant. Guerrillas who have not agreed to join have faced the prospect of severe punishment, including execution. In the case of Kenya, for example, by 1956, some 1,000 captured guerrillas had been hanged.⁷³ Similar levels of punishment were present in Rhodesia.

The most interesting factor in this “recruiting tool” is that one would expect the guerrillas who joined the pseudo units under such threats to be looking for the first opportunity to escape or to betray their teams. Rather surprisingly, instead they almost inevitably remained loyal and very effective members of their units. Despite the large numbers of pseudo missions in Kenya and Rhodesia, there

were only a handful of examples of betrayal or desertion. The lesson from both these countries was that, given good leadership and tight unit cohesion, the ex-guerrillas were every bit as loyal and effective as the government troops.

3. Coordination is critical. Coordination of the operations of pseudo teams with other military operations is critical. Two opposing requirements constantly face the planners of pseudo operations. If details of ongoing operations are disseminated too broadly, the odds of leaks leading to disclosure of team operations are increased exponentially. This clearly can result in team members being exposed and killed by government opponents. On the other hand, if pseudo team operations are held too closely, teams can be in danger from the operations of their own side. This, in fact, occurred in one operation early in the use of pseudo operations in Rhodesia.⁷⁴ In June 1978, another team was killed due to an error in coordination between operating boundaries.⁷⁵

The principal tool used in deconflicting Selous Scouts operations from those of army and police forces was "frozen areas." The official description of how frozen areas would be established read as follows:

A Frozen Area is a clearly defined area, in which Security Forces are precluded from operating, other than along main roads. Army Security Forces already in an area to be declared "Frozen" will be withdrawn from such an area by the time stipulated in the signal intimating that such an area is to be "Frozen." This signal must be acknowledged by the recipient. The above ruling also applies to all armed members of the Services and Government Departments with the exception of:

- a. Those personnel tasked to operate exclusively along the Cordon Sanitaire.
- b. Those personnel stationed at Protective or Consolidated Villages and establishments provided with a permanent guard in which case they are restricted to 1000 metres from the perimeter of such establishments.
- c. In the event of a vehicle breakdown, ambush, or mine deterioration on the main road within a Frozen Area, those personnel involved are to remain in close proximity of their transport.⁷⁶

A similar system was used in Kenya in which pseudo operations were coordinated with district operations rooms. Areas would be cleared, but reportedly "it was not easy."⁷⁷ As with Rhodesia, there were occasional breakdowns leading to security forces interfering with the pseudo teams.⁷⁸

4. Breaking guerrilla communications systems is a key tool. One common pattern for success in these pseudo operations has been weaknesses in the communications system of the targeted guerrilla groups. A key step in preparing the environment in Malaya was Special Branch's breaking of the guerrillas' primary courier system. This forced them to rely on a slower, more cumbersome system that was prone to being intercepted by the British.⁷⁹

Two aspects of the ZANLA command and control system made the operations of the Selous Scouts easier. The first was that the insurgents did not have radio communications. As a result, they had to rely on couriers, messengers, and written communications. These were slow and cumbersome, and enabled the Scouts to break into the middle of the system.⁸⁰

The second aspect was that command was very decentralized, somewhat unsurprising in many insurgent groups. This decentralization made it easier for pseudo teams to convince actual guerrillas of their authenticity. It also had a critical impact on the teams' ability to impact the guerrilla groups: "In general, the Selous Scouts achieved less success in penetrating the tighter, more disciplined ranks of ZIPRA than was the case in the unstructured command and control groupings of ZANLA."⁸¹

5. Effectiveness of pseudo operations depends in large part on the effectiveness of response forces. In both the cases of Rhodesia and Kenya, the practical impact of the pseudo teams was dependent in part on how effectively military units responded to the intelligence they provided. Certain units seemed to provide more effective military operations against the insurgents. Reid-Daly noted the key aspects of the response troops: "There are three prime qualities required of a soldier employed in fireforce duties. They are: 1. to be highly aggressive; 2. to be an accurate snap shottist; [sic] 3. to have plenty of initiative."⁸²

The Rhodesian military developed a special response force to convert the intelligence provided by the Selous Scouts into military strikes. The force was called Fireforce, and was equipped with the few helicopters that Rhodesia possessed; later it also was augmented with paratroopers.⁸³ The best unit for response in Rhodesia reportedly was the Rhodesian Light Infantry which worked regularly with the Selous Scouts.⁸⁴

Kitson also observed in the case of Kenya that members of the Kenya Regiment were particularly good at operations since all their men spoke Swahili and understood the area of operations very well.⁸⁵ On the other hand, the Kenya Regiment caused some problems for Kitson's teams since it conducted some unilateral pseudo operations designed to kill guerrilla groups rather than using them for intelligence roles.⁸⁶

Connected with the issue of response forces is how to coordinate the removal of pseudo teams once the response forces are called in. This proved somewhat less of a problem in Kenya since the response units typically consisted of elements controlled by police. As such, they normally focused on capturing the insurgents. Nevertheless, as Kitson noted, when police seized pseudo team members who had arranged for the guerrillas' arrests, they "got their share of the bruises."⁸⁷

6. The role of "turned" guerrillas is critical. There are two key aspects in the role of captured guerrillas who cooperate with the government and their effect on pseudo operations. First, even if the guerrillas are not used in the field with the pseudo teams, they are critical in providing current information on how the guerrillas operate. This can include such aspects as personality profiles of guerrilla leaders, current recognition codes and communications procedures, and general operating techniques.

Without this current intelligence, pseudo operations have no chance of long-term success. A corollary of this requirement is that the government needs a reasonably steady supply of cooperative captured guerrillas. Most guerrilla groups will change their communications and codes very regularly as a routine security measure. In many cases, these techniques will involve relatively low tech methods such

as special visual signals or dead drops. The absolute best source for this level of information is a recently captured guerrilla.

Beyond their intelligence value, cooperative guerrillas can be crucial in training pseudo teams. They can provide details of the ideological underpinnings of individual guerrillas, details of their training and customs, and habits in the field. In short, they can teach government pseudo personnel how to think like guerrillas.

The second key use of cooperating guerrillas is, of course, as members of operational teams. In some cases, it appears as though government pseudo teams have had some success without using former guerrillas, but these cases have been the exception rather than the rule. For all the reasons discussed earlier, guerrilla team members can be crucial in providing credibility to pseudo teams. If the capture and subsequent “turning” of guerrillas is handled surreptitiously, then they can be re-inserted into areas in which they have operated previously.

CONCLUSIONS

Pseudo operations have proven to be a valuable tool in several foreign counterinsurgency campaigns. In general, they have been best suited for collecting intelligence information that would be difficult to acquire through other means. When used for offensive operations, the best use for pseudo teams is to capture or kill key guerrilla leaders. The teams typically have been controlled by police services, but this largely was due to weaknesses in the respective military intelligence systems.

In the best situations, pseudo teams can enter a synergistic cycle in which their capture of guerrillas leads to more accurate intelligence which in turn results in capturing more guerrillas. Capture should always take priority over killing insurgents. Whether the captured guerrillas are used primarily for gaining current intelligence or are actually part of pseudo teams, their willing and active cooperation is essential for the success of pseudo operations.

Many of the early pseudo operations look in retrospect to be rather amateurish in terms of tradecraft. Nevertheless, they worked very well. It is likely that most guerrilla movements have become more

sophisticated in their operations; as a result, pseudo teams must also develop better techniques. The pseudo operations strategy, however, still should provide major benefits against insurgent groups.

ENDNOTES

1. Michael McClintock, *Instruments of Statecraft: U.S. Guerrilla Warfare, Counterinsurgency, and Counterterrorism, 1940-1990*, New York: Pantheon, 1992. Available at <http://www.statecraft.org/about.html>.

2. Major Lawrence M. Greenberg, *The Hukbalahap Insurrection: A Case Study of a Successful Anti-Insurgency Operation in the Philippines—1946-1955*, Washington DC: U.S. Army Center of Military History, 1995, pp. 118-119.

3. *Ibid.*, p. 125.

4. McClintock, Chapter 4.

5. Noel Barber, *The War of the Running Dogs: The Malayan Emergency: 1948-1960*, New York: Weybright and Talley, 1971, pp. 239-251.

6. *Ibid.*, p. 196.

7. Edgar O'Balance, *Malaya: The Communist Insurgent War, 1948-1960*, Hamden, CT: Archon, 1966, p. 126.

8. For a contemporary argument on the importance of this publicity, see F. H. Lakin, *A Study of Surrender Behaviour Among Chinese Communist Terrorists in Malaya*, Operations Research Section (Psychological Warfare) Memorandum No. 1/53 (declassified from Secret), 1953, United Kingdom National Archives reference WO 291/1763.

9. Frank Kitson, *Gangs and Counter-Gangs*, London: Barrie and Rockliff, 1960, p. 19.

10. For a detailed examination of British intelligence operations in Kenya, see Randall W. Heather, "Intelligence and Counter-Insurgency in Kenya, 1952-56," *Intelligence and National Security*, 5/3 July 1990, pp. 57-78. For a broader examination of British intelligence doctrine for counterinsurgency, see Keith Jeffrey, "Intelligence and Counter-Insurgency Operations: Some Reflections on the British Experience," *Intelligence and National Security*, 2/1 January 1987, pp. 118-145.

11. Kitson, *Gangs*, p. 19.

12. *Ibid.*, p. 65.

13. *Ibid.*, p. 135.

14. *Ibid.*, p. 76.

15. *Ibid.*, p. 101.

16. *Ibid.*, p. 126.

17. *Ibid.*, pp. 126-127.

18. *Ibid.*, p. 171.

19. *Ibid.*, p. 166.

20. Alf Andrew Heggoy, *Insurgency and Counterinsurgency in Algeria*, Bloomington, Indiana: Indiana University Press, 1972, p. 175.

21. For an excellent treatment of the GCMA, see Philippe Pottier, "Groupement de Commandos Mixtes Aéroportés: A French Experience in Counterinsurgency," *Small Wars and Insurgencies*, forthcoming.

22. Major Gregory D. Peterson, *The French Experience in Algeria, 1954-1962: Blueprint for U.S. Operations in Iraq*, Ft. Leavenworth, KS: School of Advanced Military Studies, p. 33.

23. *Ibid.*, pp. 32-33.

24. John Pimlott, "The French Army: From Indochina to Chad, 1946-1984," in Ian F. W. Beckett and John Pimlott, *Armed Forces & Modern Counter-Insurgency*, New York: St. Martin's Press, 1985, p. 66.

25. Martin S. Alexander and J. F. V. Kieger, "France and the Algerian War: Strategy, Operations, and Diplomacy," *Journal of Strategic Studies*, Vol. 25, No. 2, June 2002, pp. 6-7.

26. Heggoy, p. 173, argues that after 1956, "single terrorists or small cells of two or three guerrillas represented the rebels and, for all practical purposes, soon came to play the only active armed role." Although perhaps overstated, the FLN clearly was having critical command and control problems within the interior of Algeria by this point.

27. Abder-Rahmane Derradji, *The Algerian Guerrilla Campaign: Strategy & Tactics*, Lewiston, Canada: The Edwin Mellen Press, 1997, p. 204.

28. For details, see Alistair Horne, *A Savage War of Peace: Algeria 1954-1962*, London: MacMillan, 1977, pp. 255-257.

29. For details of the early period of the insurgency, see Anthony R. Wilkinson, *Insurgency in Rhodesia, 1957-1973: An Account and Assessment*, London: The International Institute for Strategic Studies, Adelphi Paper 100, 1973.

30. Bruce Hoffman, Jennifer M. Haw, and David Arnold, *Lessons for Contemporary Counterinsurgencies: The Rhodesian Experience*, Santa Monica, CA: RAND, 1991, p. 16.

31. For details on the command and control system, see J. K. Cilliers, *Counter-Insurgency in Rhodesia*, London: Croom Helm, 1985, pp. 60-77.

32. *Ibid.*, p. 223.

33. *Ibid.*, p. 71. For a detailed survey of developments in Rhodesian military intelligence, see Cilliers, pp. 224-232. Also see Hoffman, *et al.*, pp. 28-29.

34. Lieutenant Colonel R. F. Reid-Daly, *Pamwe Chete: The Legend of the Selous Scouts*, Weltevreden Park, South Africa: Covos-Day Books, 1999, p. 10.

35. For details, see Ian F. W. Beckett, *The Rhodesian Army: Counter-Insurgency 1972-1979* at http://members.tripod.com/selousscouts/rhodesian%20army%20coin%2072_79%20part2.htm.

36. *Ibid.*, p. 52.

37. *Ibid.*, pp. 56-57. Reid-Daly notes that he had to fight hard for this extra pay.

38. *Ibid.*, p. 54.

39. *Ibid.*, p. 70.

40. Cilliers, p. 27.

41. Reid-Daly, p. 302.

42. *Ibid.*, p. 276.

43. For example, 18 civilians were killed in an ambush of what was believed to be a military vehicle in Zambia in 1979. Reid-Daly, p. 462.

44. The chief of Rhodesian intelligence also concluded that these raids generally were counterproductive. Ken Flower, *An Intelligence Chief on Record: Rhodesia into Zimbabwe, 1964 to 1981*, London: John Murray, 1987, pp. 150-151.

45. For his account of the raid, see Reid-Daly, pp. 191-247.

46. For an extended excerpt of UN condemnation of this operation, see David Martin and Phyllis Johnson, *The Struggle for Zimbabwe: The Chimurenga War*, New York: Monthly Review Press, 1981, pp. 241-242. The authors, who clearly supported the liberation cause, also state that they visited the camp shortly before the raid and claim that they saw no evidence that it was anything but a refugee camp.

47. *Ibid.*, p. 105.

48. *Ibid.*, pp. 106-107.

49. Cilliers, p. 132.

50. John P. Cann, *Counterinsurgency in Africa: The Portuguese Way of War, 1961-1974*, Westport, CT: Greenwood, 1997, pp. 96-102.

51. Ian F. W. Beckett, "The Portuguese Army: The Campaign in Mozambique, 1964-1974," in Ian F. W. Beckett and John Pimlott, editors, *Armed Forces & Modern Counter-Insurgency*, New York: St. Martin's Press, 1985, p. 149.

52. *Ibid.*

53. For further details on issues surrounding the Special Teams, see Henri J. Barkey and Graham E. Fuller, *Turkey's Kurdish Question*, New York: Carnegie Commission on Preventing Deadly Conflict, 1998, pp. 148-149.

54. Reid-Daly, pp. 140-141.

55. For example, see Kitson, *Gangs*, p. 78. He also notes that in the early period of the pseudo gangs, such fines were useful since it was hard to get sufficient funds from the British government.

56. For a detailed examination of British counterinsurgency doctrine, see Thomas R. Mockaitis, *British Counterinsurgency, 1919-1960*, London: Macmillan, 1990.

57. The Rhodesian chief of intelligence also blamed an attitude shift among the Selous Scouts for supervision problems: "... the Scouts abandoned all pretensions to secrecy, attracting attention rather than deflecting it ... and emerging as the glamour boys of the Army." Ken Flower, *An Intelligence Chief on Record: Rhodesia into Zimbabwe, 1964 to 1981*, London: John Murray, 1987, p. 124.

58. Kitson, *Gangs*, pp. 185-188.

59. Frank Kitson, *Bunch of Five*, London: Faber & Faber, 1977, p. 151. For a more detailed treatment of how Kitson argues this should work in practice, see Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, and Peacekeeping*, London: Faber and Faber, 1991, pp. 95-131.

60. Reid-Daly, p. 69.

61. *Ibid.*

62. Reid-Daly, pp. 80-81, notes that in one of the first Selous Scouts operations, the team was compromised by an over zealous Special Branch officer who arrested all the insurgent contacts the team identified. The British tended to be very careful in dealing with this issue. They, in fact, reportedly did not arrest mid-level MRLA officials when discovered in hopes that they could lead to greater gains. Anthony Short, *The Communist Insurrection in Malaya, 1948-1960*, New York: Crane, Russak, 1975, pp. 361-362.

63. *Ibid.*, pp. 93-94.

64. *Ibid.*, pp. 349-354.

65. Kitson, *Gangs*.

66. Kitson, *Gangs*, p. 83. The explanation worked long enough for the pseudo team to overpower the group of Mau Mau.

67. As one example, in Reid-Daly's study, an appendix includes all the awards citations for the Selous Scouts. African Scout members were very well-represented for gallantry and service awards.

68. Cann, pp. 96-98.

69. Noel Barber, *The War of the Running Dogs: The Malayan Emergency: 1948-1960*, New York: Weybright and Talley, 1971, p. 70.

70. Robert Thompson, *Defeating Communist Insurgency: Experiences from Malaya and Vietnam*, London: Chatto & Windus, 1966, p. 88.

71. Statement by one of the principal U.S. advisors to the Philippine counterinsurgency campaign. Quoted in McClintock, Chapter 4.

72. "Kikuyu Hammered on the Anvil," *The Daily Nation*, Kenya, April 15, 2004.

73. *Ibid.*

74. For details, see Reid-Daly, pp. 22-24.

75. *Ibid.*, p. 348.

76. Rhodesian Army, Military Support to the Civil Power (MCP) (restricted, as amended, dated 1 May 1976), p. xvi. Quoted in Cilliers, p. 122.

77. Kitson, *Gangs*, p. 75.

78. For example, see Kitson, *Gangs*, pp. 150-151.

79. Barber, p. 268.

80. Reid-Daly, p. 133.

81. Cilliers, p. 126.

82. Reid-Daly, p. 366.

83. Hoffman, *et al.*, p. 21-22.

84. For details about this unit's training, see Captain James K. Bruton, USAR, "Counterinsurgency in Rhodesia," *Military Review*, Vol. 59, No. 3, 1979, pp. 32-33.

85. Kitson, *Gangs*, pp. 120-121.

86. *Ibid.*, pp. 121-122.

87. *Ibid.*, p. 165.

Protecting Ourselves

1- What assumptions does the ARRT approach make concerning the type of organization applying its recommendations? How closely does your organization fit this profile? Which recommendations are suitable for your organization? Are there recommendations here that would be inappropriate for your organization?

2- ARRT writes: "the best security conceivable won't enable a group to survive political mistakes. Effective security must be combined with correct political estimates and line, mass roots and ties, the ability to recognize and correct errors, and the ability to project a clear alternative vision of society." But also: "Acknowledging the primacy of politics cannot be allowed to slip into a faith that 'good politics' will transcend state repression."

What is the relationship between "good politics" and good security?

How does this operate at the movement, (internal) organizational, and individual levels?

3- ARRT recommends that security "be the task of the most capable, most experienced, and most politically developed members of an organization" and that "Real investigative security work within an organization must be centralized at the top."

In your study group, brainstorm a list of the strengths of this approach? Brainstorm a list of the weaknesses. How do they compare?

How does the "centralized at the top" approach fit with the requirement that "All members. . . be taught to criticize and to question, in ways that encourage exploration of the problem, any activity that raises security questions"? What does this latter capacity look like to you? How does your organization encourage and develop it?

4- ARRT warns against "a responsive militarization." Why is such militarization a problem? Can you think of examples from your own experience, or from history?

5- Describe the various types of police agents profiled in the article. What behaviors and traits do they typically exhibit? Are they problems in and of themselves? How can a group respond to these behaviors and traits when it lacks other evidence of police involvement? How can it respond when it has such evidence? How much does the question of "proof" matter? What are the dangers opened up by unsubstantiated or irresponsible accusations of infiltration or informing?

Has your group encountered such situations in the past? How was it handled?

Scarry

1- Describe and distinguish between the two models for security that Scarry describes -- democratic and authoritarian. Which does the ARRT model resemble?

2- Explain the role of time as a justification for the authoritarian model. How is this different from the reasons ARRT cites for the centralized, top-down approach? Can the democratic model address ARRT's concerns?

3- Which model does your organization's security apparatus resemble? Which is more in keeping with your organization's politics? Which is more adequate to your organization's needs? Klein

1- How do the policies Klein describes protect the people and/or the governments of the countries involved? What are the attendant risks of these policies?

2- How are the security strategies Klein describes similar to the approach Scarry advocates? What are the differences?

3- What relationship does Klein see between politics and security? How does this compare to the relationship as ARRT sees it?

Snitches

1-What does the article identify as the weaknesses in the anarchist movement that allows snitching to occur? What does it suggest as remedies? Evaluate this approach.

2- Are the weaknesses peculiar to anarchism? Is the recommended approach applicable outside of the anarchist movement?

3- Among the several approaches discussed in this article, which most resembles your organization's? Have you faced the same problems? How can these shortcomings be addressed?

PROTECTING OURSELVES FROM STATE REPRESSION
A MANUAL FOR REVOLUTIONARY ACTIVISTS

Volume One: Organizational Security

Anti-Repression Resource Team
Jackson, Mississippi

Midwest Research Group
Chicago, Illinois

Copyright 1983
All Rights Reserved
Not to be reproduced without permission

CONTENTS

ORGANIZATIONAL SECURITY.....	1
RECOGNIZING DIFFERENT TYPES OF POLICE AGENTS.....	
Deep Cover Informers	
Extraordinary Agents-Provocateurs	
Regular Informers/Provocateurs	
Passive Informers	
MOVING AGAINST INFORMERS:	
CONSIDERATIONS AND ALTERNATIVES	
MOVING AGAINST INFORMERS:	
USE OF PUBLIC INFORMATION SOURCES	
MOVING AGAINST INFORMERS:	
USE OF NON-PUBLIC INFORMATION SOURCES	
TELEPHONE SECURITY	

For information, including arrangements for anti-repression training, contact:

Anti-Repression Resource Team
P.O. Box 122
Jackson, MS 39205

601-969-2269

All movements, organizations, and individuals whose political activities are intended to bring about fundamental change in the status quo must expect to face state repression. This is the *normal* situation, not the exception, in modern capitalist society, no matter how free and democratic political life may seem.

Generally speaking, the degree of repression will be roughly proportional to the perception the ruling class and its political police agencies have of the threat posed by any particular activist or group of activists after other means of containment-such as attempts to co-opt or deflect a political challenge with apparent concession-have been considered, but not always. At times repression may serve a scapegoating function, as was the case with the extreme repression of Communists and suspected sympathizers during the McCarthy era, and thus exceed "normal" levels. At other times massive exposure and protest may beat back the ability of the police to conduct repression for a time.

The ability of activists to carry on successful political work will increasingly depend on their ability to counter state repression effectively through organizational security measures. Other volumes in this series will detail the methods of the secret police, their technology, profiles of a number of their *agents provocateurs*, and some examples of successes at countering them. Here we shall elaborate the principles of security by which groups can best protect themselves against police measures to disrupt, discredit, misdirect, and otherwise neutralize them through the use of infiltration agents and provocateurs.

Though the worst and most violent repression is normally directed against revolutionaries, that is not always the case; even quite limited demands and moderate tactics are no guarantee against repression. This being the case, security- self-defense against repression -- is needed in all progressive groups. However, the intended focus here is security for movements and organizations that are revolutionary, that do not limit their actions to the framework of legality and legitimacy of the system, but aim to overthrow it. State repression here, while including all of its general features, will also contain elements that are different in kind, not just degree. On the other hand, the radical nature of the project limits the potential of legal and political defenses, while the greater degree of organization and consciousness permit much greater vigilance.

No revolutionary group can both survive and remain revolutionary over any substantial period of time without decent security. However, the best security conceivable won't enable a group to survive consistent political mistakes. Effective security must be combined with correct political estimates and lines, mass roots and ties, the ability to recognize and correct errors, and the ability to project a clear alternative vision of society. Acknowledging the primacy of politics cannot be allowed to slip into a faith that "good politics" will transcend state repression.

There are many complexities in the relationship of good security to good politics. Paradoxes abound. The awareness that the state is a military, as well as a political, opponent, a precondition of effective security, can foster a responsive militarization which gravely weakens the critical capacity of the organization and creates a fertile ground for the operation of police spies and provocateurs. Our focus on a specific type of state repression will not permit us to go into real detail on the contradictory relationship between the conditions for good security and the development of the critical and counter-hegemonic capacity of revolutionary groups. From time to time as they emerge we will note specific aspects of the problem.

Repressive agencies are increasingly coming to question the essential stability of the societies which they defend. Their policies are predicated on the likelihood of a mass constituency for radical

ideas and subversive movements. Thus the police place a premium on dealing with potential leaderships and focal points for such movements before they consolidate and develop roots. Despite rhetoric to the contrary, revolutionary groups cannot effectively be treated as "common criminals." They constitute potential insurgents, and the appropriate response is a counter-insurgency strategy. This is explicitly stated in the basic training manual used by the repressive agencies of Great Britain and the United States, Frank Kitson's *Low Intensity Operations*.

It isn't enough for them to "expose" revolutionary politics through the various media smear measures which have been used with a greater or lesser impact in the past, since even the distorted presentation of the positions involved in such exposures might strike a responsive chord, or open up a broader debate that legitimizes revolutionary views.¹ Nor is it enough for them just to know what revolutionary groups are thinking and doing, which electronic and other technical means can accomplish quite adequately. Rather the real goal is to determine what such groups are thinking and doing, and to prevent momentum from developing that would make repression much more costly: This counter-insurgency work cannot be done effectively without human agents playing an *active* role--as we said above, disrupting, discrediting, misdirecting, and neutralizing the revolutionary group.

This is not to say that political police strategy consists simply of attempting to nip revolutionary organizations in the bud. They are well aware that such an approach would inevitably fail and simply result in new organizations and forms that might be more difficult to penetrate. Their general principle is still that elaborated in the Russian tsarist Okhrana (secret police) manual entitled *Directive on the Secret Service*:

The political police must prepare to destroy the revolutionary centers at the moment their activity is greatest and not allow their work to be diverted by dwelling on secondary undertakings.

Over the past few years many agents and provocateurs have been exposed, and more than a few have recanted for a variety of moral, financial, and other considerations.

The centrality of human agents in state repression means that the question of agent motivation becomes extremely important--the Achilles' heel of this form of state repression. This is true for all of the various types of agents which we will describe in the course of this manual. Fundamentally, agent motivation can be broken down into two elements: (1) they do it for the money, or (2) they do it out of ideological commitment. In each specific case these elements are combined to one extent or another, but to begin to understand the development of counter-measures, it is helpful to separate them and to consider the potential tensions and conflicts which they entail.

The economic motivation often puts the agent in a worker-employer tension with the repressive agency. Not only is there the question of the wage, but job security, safety, working conditions, etc., are all, based on the evidence, likely sources of tension. On the other hand, greed and career advancement motives of a typically entrepreneurial sort are also involved.

Ideological commitment raises a different type of problem. It is difficult to internalize political views to which you are hostile in principle. More important, just as people generally are susceptible to ideological breaks, so are agents. Indeed their intimate connection with a movement and with individuals who are convinced that what they are doing is right and who are generally decent people places huge strains on their own commitment as well as on their psychological stability.

¹ Thus in Ireland, both "free" and occupied sectors, the media are forbidden to broadcast any Sinn Fein views. Northern Ireland is capitalism's current testing ground for the most modern forms of "democratic" repression.

The very temporary official reaction against political police and their abuse of authority during the post-Vietnam/Watergate period, and the anti-Red Squad/FBI/CIA/Military Intelligence revelations which followed, not to mention such exemplary actions as the Media, Pennsylvania, document liberation which first revealed the FBI's COINTELPRO operations, have been invaluable sources of information. There is still a problem that various left groups refuse to admit, even to their own memberships and certainly not beyond them: the extent to which they were penetrated and influenced, and what allowed it to happen. But despite this there is sufficient mobility among leftists that essential details can be discovered by those who expend the required effort. All of this put together has resulted in a substantial body of knowledge on the subject. It is safe to say that there is a "state of the art" consensus on the detection and neutralization of agents. This volume is an attempt to summarize it.

Security must be the task of the most capable, most experienced, and most politically developed members of an organization. Younger or newer members very seldom have the depth of experience necessary to understand the various clues that lead to suspicion then belief that there is "something wrong" going on. Often the clues themselves are political: failure of a member to develop politically; someone changing political position for no observable reason; disruptive suggestions; failure to work up to political potential; etc. Real investigative security work within an organization must be centralized at the top.

However, *the experience should be of a non-sectarian character that would allow for communication and relationships across political divisions, and be in a variety of conditions and frameworks.* It is no place for one whose political experience and credentials are substantially defined by loyalty to the leadership. Otherwise, since leadership often has a personal stake in discussions of organizational security -- they are responsible for the influence and access of agents; their political and personal judgement is in question -- centralization of security in the wrong people, even those with considerable experience, can play directly into the hands of the police.

All members and followers of an organization should be taught to criticize and to question, in ways that encourage political discussion of the problem, any activity that raises security questions, even when doubts are based on fragmentary evidence. All potentially damaging incidents should be reported to one or two leading members of the organization. Too often a group has learned in hindsight that they could have known that something was happening had some of the members only reported what they observed at various times to one person who could have detected the pattern of what was going on. In this respect, members should understand that security is everyone's concern. Thus anyone whose address book suddenly disappears should recognize and report a security problem, for example. As all damaging incidents, strange/unusual events, and rumors are centralized, a log of all such happenings should be made with as much detail as possible. Dates, names of persons involved, reporting person, what took place, and what was the effect of the happening should be carefully recorded in the log.

While political questions and concerns should be generalized so that members can participate fully in discussions and decisions, matters that must be handled covertly should be compartmentalized and limited to those members who have a "need to know." When informers/provocateurs are thrown out of the organization, they should know only a part of what was going on in sensitive areas. That part compromised by an informer's knowledge should be disbanded immediately and reorganized in a different way. With tight compartmentalization, an informer will know only a fraction of the secret information. If an informer knows all or most of an organization's secret activities, the organization itself may have to be disbanded. But this only works to the extent that the amount of such "secret" information, known only to the very top leadership and to the members directly involved, is minimized. Those for whom everything is secret usually manage to keep very few secrets.

Even illegality is not necessarily a matter for secrecy and compartmentalization. Some of the most effective direct actions of recent years have been planned and discussed openly. But an action that could be thwarted by police foreknowledge, or that could easily be deterred by provocation, should be treated as a security matter for as long as necessary.

As people become more important to the organization, the organization should know all or most of the person's background. For certain group functions, a routine background check should be made. This is especially true for people who have no identifiable roots. Where did they come from? With whom did they interact politically? The greater the group responsibility given to an individual, the more need there is for a detailed background check.

The clearest example of such a need is that of Douglas Durham, a white man who posed as an Indian and infiltrated the American Indian Movement from March 1973 to March 1975. Durham had NO previous movement experience, was involved in several embarrassing and well-known law enforcement scandals in Des Moines, Iowa; was well known as a front man for organized crime; and had administered a severe beating to his wife from which she died shortly thereafter. Asking for Durham's life history and work record, and investigating it thoroughly, would have turned up some or most of the sordid past of Durham's life. Instead, Durham was appointed AIM's national chief of security, coordinator of the Wounded Knee Legal Defense/Offense Committee, and director of the new national AIM office in St. Paul, Minnesota. For lack of a check on Durham's background, AIM had an FBI informer/provocateur deeply imbedded in the national leadership and running the day-to-day operations of the group, as well as its security.

One of the greatest needs of any revolutionary organization is explicit knowledge of the tactics and strategies of the repressive organizations of the state. At least one or two people in the organization must be delegated the task of learning about the FBI, CIA, Treasury Department, local police, and military intelligence. Learning about the repressive agencies means reading and more reading from all sources about past actions of the intelligence agencies that have been exposed in the media. Learning may also mean interviewing members of the repressive agencies who are willing to talk for various reasons. Remember that in the 1960s the repressive forces knew plenty about the Movement and the Movement knew nothing about the repressive forces. Will the Movement remain stupid forever? Remember, if a Weatherman does not know which way the wind is blowing, somebody else has got to know. We think that the Movement *must* know!

By the same token, it is important to understand that the police are not invincible, and that there is a considerable amount they rarely understand. One reason the state sees conspiracies everywhere is because it cannot comprehend why people act radically. Thus throughout the sixties and early seventies, the intelligence agencies searched vainly for some foreign power responsible for the radical insurgency in the U.S.

RECOGNIZING DIFFERENT TYPES OF POLICE AGENTS

There are four basic types of agents the police infiltrate into radical movements: deep cover informers, extraordinary agents-provocateurs, regular informers/provocateurs, and passive informers.

Deep Cover Informers are agents of the State who are usually regular employees of the repressive agencies, such as Cril Payne, an FBI Special Agent who attempted to infiltrate the Weather Underground. Payne was one of half a dozen regular FBI Special Agents who were given entire fake

identities, planted in various movement groups to gain movement credentials, and targeted against the remnants of the Weather Underground. Such agents are usually given "backstopped identities," which means that they have an entire fake background that will check out all the way along. Often they are "sheep-dipped" as well, meaning that they have been placed in a Movement group for some period of time, and done good work, so they have real "Movement Credentials" as well.

Deep cover informers also arise out of two other situations: (a) Often they are members in good standing in responsible positions who have lost credibility or become embittered by one or more organizational decisions and turned against the group. The FBI contacts them or they contact the FBI and make known their anti-group feelings, and after an FBI check they are often ordered to stay in place. They do good work, contribute to the organization's political life, and are regarded as good and righteous comrades. The classic case is the Childs brothers, one of whom was editor of the Communist Party's *Daily Worker* and then got demoted as a result of an intra-party struggle. At this time, the early fifties, both brothers became FBI informers until 1980, when they were exposed in David Garrow's book, *The FBI and Martin Luther King, Jr.: From "Solo" to Memphis*. The Childs brothers (code-named "Solo" by the FBI) operated at the highest levels of the Communist Party for 25 years. (b) Sometimes the FBI can catch young recruits and turn them over through threats, coercion, or fear. Once in the group, the young recruit-informer may ascend to a leadership position.

Deep cover informers, then, are either agents of the state with secure fake backgrounds, often sheep-dipped, *or* they are cadre members turned in place, *or* they are young recruits turned early by the state who ascend the leadership ladder of the organization. They are difficult to spot because they contribute as much to the functioning of the group as do regular members, *or more*.

It is our opinion that such informers are rarely caught unless they show symptoms akin to other types of informers. The only effective way to identify such informers is through Counter-Intelligence (CI), discussed below.

Extra-ordinary Agents-Provocateurs are individuals who are agents of the state, although not usually regular employees, who make a living out of destroying ongoing movement organizations by disrupting and factionalizing a group to an extraordinary degree. These individuals are extraordinary action people, ready to deal with guns and armed struggle, ready to participate in direct action in all its forms and to be arrested. They are often noted as people who get things done that nobody else can do, i.e., get information about police thinking/action, background information on individuals, etc. Because of their extraordinary capacity for action and their courage in doing the actions, these individuals usually gain easy access to top leadership in the group. Of course, since they are agents of the state, these agents-provocateurs also have spectacular failures in getting things done, and usually these failures happen at especially crucial moments in the life of the organization.

One of the telltale signs of an extraordinary agent-provocateur is the advocacy and use of excessive violence. Doug Durham, who infiltrated AIM, was extremely violent towards women, and personally engineered a building takeover in Des Moines with eight armed Indians in August 1973. The armed Indians represented Des Moines AIM, and as a result of the takeover, AIM was discredited in Iowa. William O'Neal, the FBI infiltrator in the Illinois Black Panther Party, built a working electric chair allegedly torture members accused of being spies for the state. Although the Panthers never used the chair, even its existence discredited them, and frightened the Panther cadres. Quite often, extraordinary agents-provocateurs gain their initial respect by procuring guns for a group. Others constantly urge the groups on to violent confrontations or armed actions which will be counterproductive.

Extraordinary agents-provocateurs are usually very close to one or more top leaders and make sure they get along well with them, But they are generally very difficult for others to get along with. Their usual social behavior is bad to atrocious except when leadership is around. Durham's extreme anti-social behavior, especially his violent male chauvinism, bending women to do what he wanted, was well-known within AIM, but he was never confronted with it by the AIM leadership, Durham had been a close friend of Dennis Banks, one of the top leaders of AIM, for two years. While Durham was given assignments such as Security Director nationally for AIM, and leader Banks accepted none of the criticisms of his behavior, other members of AIM, especially women, had complained of his abusive and arrogant behavior for a long time. Essentially, AIM leadership shielded Durham from charges of socially disruptive and male chauvinist behavior. The same point should be made about O'Neal who was close to Bobby Rush, the BPP Minister of Defense. O'Neal was known to attack women sexually, including BPP female cadres, and engaged in a series of anti-social actions such as doing stickups and firing a gun during a BPP meeting, as well as building the electric chair.

It is important to understand that the special relationship of the extraordinary agent-provocateur with one of the top leadership in the group may lead to very damaging factional fights and to demoralization and disintegration of the group. Durham factionalized AIM by preventing other leadership people and other members from gaining access to Banks. Many were embittered by this fact alone. In addition, Durham belittled and disparaged other legitimate leaders, causing them to lose credibility in the group. Durham was able to get Banks to commit AIM to an action that everyone else opposed. Thus Durham was able to split AIM by accenting personality conflicts between top leadership and others, insulating Banks from much of the group's persistent criticism, and falsely criticizing other leaders and members as a spokesperson for Banks.

Fred Hampton was skeptical of O'Neal, and according to some sources wanted O'Neal put out of the party, but the criticisms from Hampton and others were soft-pedalled by Rush. Rush wanted a practical man of action in the party and held on to O'Neal despite major pointed criticisms of O'Neal's behavior. This situation led to a major problem, but unlike the AIM situation, Hampton was able to isolate O'Neal's poisonous effects and Hampton continued to inspire the Panthers. No doubt the failure of O'Neal's efforts to factionalize the Illinois chapter enough to disintegrate it led the FBI to plan and carry out Hampton's assassination.

Extraordinary agents-provocateurs are extremely disruptive politically. Very often their political lines change abruptly, without apparent reason or explanation. Quite often these changes of line are meant to encourage the growth of deep and vindictive faction fights within the group and/or to encourage deep divisions between various groups. Disruption often takes the form of outright lies to others. O'Neal, for example, told various lies to the Blackstone Rangers and the BPP in order to break up a budding alliance. Perhaps the alliance would not have flowered anyhow since it was against the basic interests of the leadership of the Rangers, but the lies probably deepened the Panther/Ranger split far more quickly and with more hostility than had things broken off more naturally. Publicly putting down other groups often engenders hostilities that shut off the delicate political process of cooperation between groups. An extraordinary agent-provocateur very often will misrepresent the group's position when sent as a representative to a conference. Joe Burton, an FBI informer and regular agent-provocateur, was instructed by the FBI to disrupt the unity conference of the Revolutionary Union and the October League by pushing ideological stands that would make unity impossible. Burton would also insult the people whose stands were for unity by making up false accusations on the spot. We are not sure whether unity could have been achieved even without agents and provocateurs, but it is clear they made the delicate process of unification many times more difficult.

Along with the political disruptiveness is a basic lack of solid political growth. When long experience with a particular issue does not lead to qualitatively better political understanding of the issue, there are grounds for security suspicions. Extraordinary agents-provocateurs are usually action-oriented and press ahead with more daring and more illegal activities without any increase in their political understanding of an issue. Bill Frapolly, a Chicago Police Department cadet, graduated from a fairly tame college SDS group to the Weatherman faction without being able to explain politically why he had made such a heavy leap in activism. Most are basically unable to justify their actions on political grounds and therefore their political ineptness has to be shielded in some way. Some of the Panthers let O'Neal slide by saying that he was a "lumpen" (or street person) whose political instincts were sharp. No demands were made on O'Neal to become articulate and to grow politically. Doug Durham was a non-participant in the AIM strategy sessions where policy was being made. Durham would stand on the fringes of the discussion room or out in the hall, never putting in an opinion as to the next step to take organizationally.

Extraordinary agents-provocateurs are usually also disruptive in regard to group money. Mishandling of group funds creates powerful hostile membership feelings within a group and sows a basic distrust of the leadership. Extraordinary agents-provocateurs relate to money for themselves above all else. Doug Durham routinely misappropriated AIM's money and often spent it on personal goods for himself. William O'Neal committed a series of robberies using Panther vehicles, often on the way to BPP meetings with others in the car waiting as he robbed a motel or store. Tom Mosher ran heroin across the Mexican border while a courier for the Panther national leadership out of Oakland. O'Neal had FBI protection at the time of his crimes. He received only \$300 a month from the FBI for his work infiltrating the BPP, but he had protection against any law enforcement attempting to make him accountable for his crimes. The protection against prosecution, then, was the real payment from the FBI. Mosher was apprehended by law enforcement for narcotics violations and was turned into an informer/witness for the FBI and others. Mosher's criminal behavior was an obvious security risk and a clue that his politics were not firm enough to be trusted with sensitive tasks. Both Durham and Louis Tackwood, a Black provocateur in California whose activities are described in *The Glass House Tapes*, had connections to organized crime during the time they were politically active. Criminal behavior, unauthorized by the group, is a major security risk.

The last major clue about extraordinary agents-provocateurs is their travel patterns. Doug Durham finally aroused the suspicion of AIM because he was forced by the CIA to take trips to outrageous places like Jamaica. Even Durham's extraordinary ability to lie his way out of situations was overtaxed in this situation. Why should an American Indian suddenly have to take off to an exotic foreign country? Where would Durham come up with the money for such a trip? A similar situation arose when a "former" contract CIA agent surfaced in Chicago to testify on behalf of a comrade from a right-wing group. The CIA man appeared out of nowhere after jumping bond and disappearing for five years. Right in the middle of an enormous legal tangle around his buddy from the right-wing group, the CIA man took off on a six-week "vacation" to Jamaica just at the time the U.S. was trying to destabilize the Manley government. To certain observers, this was a powerful clue that the "former" CIA man was still with the Agency.

Regular Informers/Provocateurs have many of the same characteristics as the extraordinary agents-provocateurs except to a lesser degree. The regular informers share the following with them: male chauvinism, anti-social behavior, disruptive behavior, lack of political growth, and inconsistencies with regard to their political lines on various issues. Usually the regular informers are far less flamboyant than the extraordinary agents-provocateurs and look far more like regular members in their

actions.

Regular informers tend to be critical of leadership and use various means of discrediting legitimate leadership. Bill Frapolly, a Chicago PD agent and later a cop, used several tactics to discredit SDS leadership where he went to college. Frapolly started a "friendly" wrestling match with an SDS leader that turned into a real fight at a party. He organized a grouping of ex-SDS members to protest the leader's insistence that members function politically and lay off drugs. He persuaded the group of ex-SDS people that the leader was acting in an authoritarian way by cutting off people's personal freedom. Frapolly also insisted that the leader was not action-oriented enough and insisted publicly that the SDS chapter initiate direct action to get things moving. When asked by leadership to state *why* such actions should be initiated and what the politics of the actions would be, Frapolly was unable to answer convincingly and therefore discredited his own suggestions.

Another clue to regular informers is what might be called social discontinuities. One indication is the refusal to allow others to see his or her living quarters. Often the reason is that a spouse or live-in friend is non-political and would give away the game. Russ Trunzo, a CIA agent in a Chicago draft resistance organization, gave long explanations to other draft resisters as to why he was unable to have them come to his home. Police agent Frapolly lived with his family and was never able to bring movement people home. Frapolly also had a straight girl friend who told people that he was a cop, only to be disbelieved. Richard Thompson, an alias for a Chicago PD infiltrator, never allowed his comrades to come over to his place. Thompson's major push within the movement was social, to date and sleep with a woman who was at the center of many group activities, and who gossiped incessantly. Mort Frankel, a Chicago Red Squad cop and infiltrator, would not allow anybody to visit his home or know anything about his family.

Many male informers and extraordinary agents-provocateurs use sex and exploitation of women as a regular way to further their ends. Doug Durham managed a string of prostitutes in the Des Moines, Iowa, area, prior to becoming an FBI informer in AIM. Durham married one of his "girls" three weeks after his beating caused his wife to die. At major AIM events, Durham arranged for prostitutes to sleep with AIM leaders to obtain information. Durham used seduction and brutal physical force to keep Jancita Eagle Deer as an accomplice. Gary Rower, an FBI extraordinary agent-provocateur in the Ku Klux Klan, was ordered by the FBI to sleep with the wives of Klan leaders as a way of disrupting the Klan. William O'Neal participated in near rapes of female BPP members. Ron Porche, a Chicago PD informer, deliberately slept with the woman who was vice president of a Puerto Rican college group in order to gain quick access to an inside source. Female informers and provocateurs very often use sex as a way to quickly gain access to leadership of a group.

The deliberate use of sexuality is aimed at provoking sexual jealousy. A large part of group functioning can rather easily be disturbed by jealous males fighting over a seductive woman or two women fighting over the attentions of a wandering male. The real problem with the use of sex by informers is that it may not stand out as anything different from what is done by others in the group who are just regular members. Every group goes through periodic crises around who sleeps with whom, and the large majority of such incidents are not initiated by informers/provocateurs.

Regular informers often lie down on the job, fail to get organizational work done, and tend not to advance the group politically. The police agent who ran the mimeo machine for a local SDS group consistently made the leaflets come out illegible. Richard Thompson did no organizational work at all, just came to meetings and socialized with his source afterwards.

Another clue to regular informers is that they are apt to be functioning in many groups, or at least attending a vast number of qualitatively different movement functions. Some movement people have many legitimate movement interests, e.g., civil rights, political theory, anti-repression, women's movement, labor movement, etc., and can explain these interests at length. This is no problem. The problem (and clue) is when there is multiple group affiliation to groups with diametrically opposed points of view. One local Chicago infiltrator, Steve Starkweather, was functioning in the youth groups of the Socialist Workers Part, the Communist Party, and the Spartacist League simultaneously. The divergencies among these groups is so large that only a spy would function in all of them simultaneously.

Regular informers often push their interests far beyond their political capacity. Quite often informers are at events that they cannot understand or explain politically. Questions about why the potential informer would be interested in the event should be asked. Often the inconsistency is glaring between the advanced level of the event and the very low level of comprehension by the informer. Richard Thompson turned up at an advanced Progressive Labor Party event without the slightest knowledge or political interest in the substance of the conference. Bill Frapolly became a Weatherman cadre even though his understanding of political issues was rudimentary.

One particular subgroup of regular informers/provocateurs is what might be called "losers" or "crazies." These are people who are severely disturbed, often psychotic, who apparently malfunction in every area. These people include the social isolates who have no friends and are actively rejected by most or all of the group. Also included are people who are unable to complete successfully even the simplest tasks without botching them up. One would think that the FBI and other intelligence agencies would stay clear of them. But the fact is that losers, social rejects, and disturbed psychotics are easily persuaded to do the dirty work of the repressive agencies because they get heavy ego gratification by identifying with a strong, winning government agency that obviously has real power. At long last the losers have found a winner!

The classic example of a disturbed, clearly psychotic FBI informer is William Lemmer, a Vietnam veteran who infiltrated Vietnam Veterans Against the War (VVAW). The FBI deliberately manipulated Lemmer's psychotic fantasies in order to keep him in VVAW as long as possible. Lemmer actually believed that he was invulnerable to arrest and that he was *helping* VVAW by being an informer. Timothy Redfearn, an FBI informer used against the Socialist Workers Party in the Denver area, was mildly disturbed, but a definite loser type. Both the FBI and the SWP agreed that whatever Redfearn turned his involvement to "turned to shit." Political groups often tolerate such folks because they feel guilty about rejecting anyone so clearly damaged by society. Loser/disturbed types are easy to spot; the problem is what to do with them. Since they contribute little to group functioning, and they are always vulnerable to pressure and/or flattery by the repressive agencies, the group should move to put them out.

Passive informers are a regular and normal kind that the intelligence agencies use for a variety of reasons. Passive informers are usually instructed to collect personal information as contrasted to political information. Usually only a passive informer has enough personal closeness to members to learn their personal likes and dislikes, their personal animosities toward other members, their sexual preferences and deviance, and even their health problems, including physical weaknesses and handicaps.

Furthermore, handwriting samples, photos, diaries, address books, and other personal material can easily be stolen. This material is then forwarded to the FBI laboratory for potential use in

disinformation and disruption programs. For example, forgeries of letters are standard procedure in the FBI. We should note carefully the successful "snitch jacket" that the FBI placed on Bill Albertson, director of the New York State Communist Party. Also, passive informers can be used to check out the performance of other, more aggressive agents as to how well they fulfill their intelligence roles and what kind of impression they have made on key members of the group. Passive agents can be expected to last a much longer time than other types, and they can always be activated into provocateur roles using as a cover their lengthy period as passive members; most groups are delighted when a passive member suddenly becomes active and of more apparent value to the group.

The fact that most radical organizations -- including many that fight vigorously for women's liberation -- reproduce the sex role differentiation of the larger society, provides openings for the police. The passive agent role often includes large sex role differences. Female agents can be non-political, or political at a very low level, if they fulfill certain social functions well without drawing suspicion. These functions may vary from sex to cooking to child care to speaking to the social unity/social alienation of the group members. Male agents, on the other hand, are usually expected to meet a minimum level of political sophistication before they can gain group acceptance. Moreover, male agents are expected to do a minimum of real political work, and they are not allowed to substitute social functions for it. In at least one instance, the infiltration of two deep cover male agents into the Van Lydegraf Weather Underground group on the West Coast, the agents were ostensibly super-feminist men who were otherwise relatively uninvolved politically but who always fulfilled the social functions such as baby sitting.

Female passive agents typically stress social unity and completely distance themselves from political issues, arguments, and controversies. Not only is their pose non-political, but there is in reality a pronounced lack of political development. For all intents and purposes the female agent has been a social groupie whose information collection was based on social mobility and friendships within the group. The classic female passive informer, an FBI informer, was Fat Annie, who participated in several Washington, D.C., antiwar groups during the 1960s. Fat Annie was always "loving" people and demanding that the group "love" her in return. Activists felt sorry for Fat Annie and would engage in lengthy conversations with her, responding to her explicit social demands. Fat Annie was a social outcast, and the social change groups felt guilty at the prospect of rejecting her socially as the larger society did. But the crucial question was never asked or acted upon: Why was Fat Annie not rejected by the groups on political grounds? She never developed politically and was never challenged to do so in order to remain in the groups.

A final point about female passive informers is that they are frequently instructed to disrupt by criticizing the group's social functioning. Criticisms include not enough respect for individuals, not enough help with personal problems, too much group social alienation, too much politics, etc. Fat Annie was known to make all of these criticisms. While such criticisms seldom break up a political group, they tend to unsettle group members and make them feel that the group is the largest cause of various social problems within the group.

Male passive informers also rely on friendship to penetrate the group and gain information, but their mode of operation is usually different. The passive male informer must socially connect to somebody important to the group in order to have a minimum of group approval. This is achieved, for example, by sexual intimacy with a highly approved female, or by being good friends with a male leader. Ernie Sanchez, the cover name for a Los Angeles cop, started sleeping with an important female supporter of the Revolutionary Communist Party, and thereby gained entry into some leadership circles of the RCP.

Male passive agents, like the female ones, typically avoid political work and political debate but are usually reluctantly forced to do some political work in order to meet minimum group demands. Sanchez fended off attempts by RCP cadres to engage in deep political discussion and thereby garnered some suspicion from RCP members. But they always put pressure on him to do RCP work, to the point that he was forced to sell the RCP's newspaper in public in order to keep his credibility.

In order to maximize his observation of his prime target, Sanchez had to become a relatively strong, willing worker *and* he consolidated his social position by moving in with the RCP supporter he had been sleeping with. In order for Sanchez to be next to his target, Damin Garcia, who was an RCP leader in Los Angeles, Sanchez upped his work commitment to the point where he became an agitator during the RCP May Day 1980 event. RCP observers say that Sanchez was so provocative as an agitator during the May Day confrontations that he gave the LAPD an excuse to arrest the entire group savagely. Clearly, Sanchez shed his passive agent role and slipped into the role of a regular agent provocateur. Since Sanchez disappeared immediately after May Day 1980, the inference is that LAPD intended for him to play a limited passive role until his chief target was neutralized, and then to pull out.

The key to passive informers is that they must trade on social, not political, relations within the group. This means that obvious social mismatches are suspect, as well as relationships of hugely unequal political commitment where the uncommitted use the relationships to deeply ingratiate themselves into the group. When this happens, the appropriate response is for the group to demand political work and political growth from that individual. Should the individual persistently resist such demands, while maintaining a group position close to sensitive work, the individual should be thoroughly investigated. No individual in a cadre political group should be allowed to maintain membership solely or primarily on the basis of social relation.

The passive informer is in a good position to spread false rumors about members and leaders of a group. Since much of the content of a passive informer's conversation will be social gossip about group members, it is easy to slip in a series of suspicions regarding a particular group member. During periods of intensified attack on an organization, especially when it is clear that information about the group has leaked out to one or more intelligence agencies from a source or sources within the group, the police or FBI often seize the opportunity to falsely label a group member as an informer. The result of a successful "snitch jacket" is horrendous for group functioning: the most dedicated are under suspicion while the real informers go undiscovered. A clear case of a snitch jacket was that of Anna Mae Aquash, a Nova Scotia-born Indian who rose up through the ranks of the American Indian Movement to a position of leadership. The important detail to note is that John Stewart, aka Darryl Blue Lake, had spread rumors that Aquash was an informer and not to be trusted, during a time of heavy FBI investigation and harassment of AIM and Aquash during the spring of 1975. While these rumors were discounted at the time, they eventually were believed as a result of some clever FBI COINTELPRO maneuvers. Nobody had tracked down the source of the rumors until Stewart was shown to be an FBI informer in mid-1976. This was far too late for Anna Mae Aquash, who was murdered in early February 1976. Whether knowing the source of the false Aquash rumor would have prevented the snitch jacket is impossible to say, but some diligent investigation of Stewart during the time he was spreading the rumors might have yielded clues to his informer status. We should further note that rumors can be spread by any type of informer, and that investigation as to the sources of such rumors is a must for good security work.

MOVING AGAINST INFORMERS: CONSIDERATIONS AND ALTERNATIVES

Assuming that the security people within the group have suspicions about a group member being an informer/provocateur, it is useful for security/leadership to resolve certain questions both before and after the investigation:

(a) How badly do you want to know whether the person is an agent or not? Clearly, if the person under suspicion is relatively important to the group's functioning, then leadership must know one way or the other. The more important the person under suspicion is to the group, the more intensive the investigation. We may suggest methods of investigation which are unorthodox and from a certain point of view morally indefensible. But the question is always how badly the group needs to know. No group need use all or any of the methods we describe. But under the condition that the correct information is a life-and-death matter for the group, certain drastic measures may be justified.

(b) What will be done if the information is inconclusive? Often there is not enough evidence to confirm that someone is a police agent, but there is enough evidence to confirm certain suspicions. A great deal will depend upon what is at stake with the person under suspicion. In general, the choices come down to (1) labelling the person a security risk and acting accordingly; (2) doing nothing outwardly but continuing the investigation; (3) isolating the person from sensitive work but keeping him or her in the group; (4) moving to a higher stage of investigation.

(c) What will be done if the person does turn out to be an agent? While common sense dictates that the person be exposed and severed from the group, other actions might be initiated. If the presence of the agent is a real threat to the group, then the agent should be neutralized in an effective manner. Usually wide exposure of the agent will accomplish an effective neutralization. *But* if the agent is no great threat to the group's functioning, the agent staying inside the group may be useful for other purposes. Leadership might decide that they prefer to keep the agent, rather than risk not knowing who would replace a known quantity. If the agent is not in a sensitive position, can be monitored and isolated from important work, leadership may want to keep such an agent at a low organizational level. *Or* the agent might be given tasks that seem to be sensitive but are in reality not crucial to the group. Under the cover of doing "sensitive" work, false and semi-false information about the group can be relayed to the intelligence agencies that the agent belongs to. *Or* perhaps certain information that is in fact true about the group can be willfully discredited by creation of pseudo-events and/or false information. Remember that when the intelligence agencies have a great deal of contradictory information, it decreases their ability to act decisively against the group.

(d) What are the responsibilities to other groups of the group's knowledge of an informer? If the group makes a decision to sever connection with the agent, it is certainly the group's responsibility to quietly contact leadership in other groups to warn them about the agent. Often public exposure is done through the group's newspaper/newsletter/journal; in this case the news article should be sent to a wide variety of groups.*² The more pressing problem is the instance where there are only suspicions but not decisive evidence. Experience has shown that suspicions are taken seriously only when there is a political bond that exists between persons with long movement experience. People who have been in the movement a long time, and who are known to each other and trusted as dedicated movement people, can convey agent suspicions that will get a favorable hearing or be readily believed. This "old hands trust network" is relatively independent of political point of view; veteran leaders of rival radical organizations can freely and easily exchange information on matters of security.

2 Exposing agents may be a violation of the INtelligence Identities Protection Act of 1982.

MOVING AGAINST INFORMERS: USE OF PUBLIC INFORMATION SOURCES

Elsewhere we will discuss the various ways in which public records and public information can be used to investigate a potential informer. These investigations should be done without the knowledge of the subject. When information from the secret investigation is insufficient or inconclusive, questions could be put to the suspected person about cloudy or missing parts of his or her background. The questioning should be done in one session and checked as rapidly as possible to prevent the person from rigging some answers that s/he can get to check out.

MOVING AGAINST INFORMERS: USE OF NON-PUBLIC INFORMATION SOURCES

If all public information sources check out, or nothing definitive arises from this kind of investigation, there are other methods that might need to be used. In many cases they are, unfortunately, variations on methods used by the repressive police agencies themselves- fighting fire with fire, so to speak. Again we caution that an assessment must be made as to how badly the group needs the information. The non-public methods are difficult and often time-consuming and are best used when the need to know is rather high. Assuming a decision has been made that there is a great need to know if a particular person is an agent, we suggest some of the following methods:

An agent's living quarters usually contain all kinds of useful personal information. Gaining entrance by whatever means, an examination of personal papers, clothing, reading material, dope and liquor should reveal some interesting clues as to which side the person is really on. Mail is particularly important as a source of personal/political information. Rich clothing on a professed poor man's budget would be revealing. Any questionable receipts, money order, checks, etc. should be noted. Personal papers, diaries, etc. should be scrutinized for manipulations of people in the group, especially persons the subject is close to. Reading material should be checked for inconsistencies, e.g., conservative/reactionary reading material for a so-called radical. Check especially the bathroom literature, since it is most likely read. Excessive dope or liquor should be noted, since often the psychological strain on a spy is high.

An effort might be made to steal the two most vital sources of personal information, the wallet and the address book. Both of these could be demanded in a pressure confrontation (described below), but secrecy would be maintained far better if the suspect thought they were lost. Occasionally, a situation can be arranged so that these objects can be viewed without being stolen; for example, a swimming group leaves their clothes in a locked car and while the suspect swims, a confederate opens the car up and locates the desired objects. Address books are particularly desirable; every unknown phone number should be checked out. Usually agents phone in their information to their agency handler, hence an agency phone number is handy as well as the personal home phone number of the handler. Wallets are usually full of personal papers which should be noted and perhaps checked on. Quite often the wallet is also the person's address book, with small pieces of paper covered with phone numbers and/or addresses.

A very useful device to apply to a phone is called a pen register. A pen register automatically records the numbers of incoming and outgoing phone calls. It does not record conversations, but it does give a revealing record of who called the suspect and whom the suspect called. If you have an inside source within the local telephone company who has access to telephone records, that person can easily get a copy of all outgoing calls from the suspect's phone. Your inside source could also easily identify whose name and address goes with whose phone number. Or you can check them out yourself by using

the cross-reference directory in your public library or the system that authorized Bell employees use - the CN/A (Customer Name/Address) numbers. Call the CN/A number at the unknown number's area code and ask the operator to identify the name and address of the customer. The service includes businesses and non-published numbers. *Tap* suggests a call like this: "Hi, this is Jim with the Residence Service Center in Pasadena. I've got a customer on hold who claims not to have made a rather lengthy call to (212) 555-1212." *Tap* says that, "When the employee sounds natural and is cheery, the CN/A operator doesn't ask any questions" These are the known CN/A numbers:

(chart with phone numbers)

Other non-public sources of background information and how to sue them will be recommended on a case-by-case basis.

There comes a time when leadership may decide that a direct confrontation is needed to assess the suspect's reactions and obtain follow-up information. However this kind of confrontation is arranged, it puts a tremendous amount of pressure on the suspect, innocent or agent. The best way to handle this is to be matter-of-fact in requesting information. The information that is most needed at the moment and can be checked out with reasonable speed is the information you are after. Whatever is asked about - family ties, employment or military service histories - try to verify it as speedily as possible. During these confrontation interviews, standard procedure is to ask for wallet and address book. Look both over very carefully, copying down useful facts and numbers. Ask the suspect about anything suspicious or unusual and write down the replies. REMEMBER that a wallet will contain articles from a person's long ago past, so everyone is likely to have some strange items in his or her wallet. Ask all questions on the spot and conclude the interview by returning the wallet and its contents as well as the address book(s). Protocol demands that you thank the person for cooperating, and explain that you will notify him or her about the results as soon as possible, hopefully within a week's time.

A long-range goal in dealing with informers is the use of counter-intelligence. The movement has within it some of the best and brightest. What we need is to put some intellectual effort into the task of learning what goes on inside the intelligence agencies. We need contacts within all of the political police agencies who will tell us what we need to know about their operations, including informers. We believe it would be invaluable if various groups gave serious thought to infiltrating the agencies of the U.S. political police. Since the political police know a great deal about the movement, we need to know a lot more about them. We need to know what information about us is in their computers and files. The national mob killed 22 top mob leaders between 1971 and 1979 because through counter-intelligence they found out that these men were FBI informers. We are not the mob, but the fact that the mob found out means that it can be done.

TELEPHONE SECURITY

The basic rule for telephones is that they are all potentially tappable. Whether it is a crude tap in the phone box in the basement or a quickie with alligator clips in the box on the telephone pole or the sophisticated central taps that Bell Security does for the FBI, the fact of the matter is that no device we can buy or construct will prevent the political police from tapping the phone. Only if you are completely underground can you assume that your line is untapped; but of course, you will be calling other numbers that are probably tapped.

Telephone tapping, however, is a great drain on personnel time of the political police, so there are variants to the tapping game. Only real targets are tapped *and* the phone recordings listened to. In

general, the number of targets (including organized crime, white-collar crime, and ruling class business) has to be relatively small. Political targets are usually groups that know, or should know, that they are COINTELPRO targets of some sort. All Marxist-Leninist and revolutionary nationalist groups are targeted, at least the office phone and usually those of leaders as well. Any group known to practice civil disobedience, direct action, self-defense, or revolutionary armed struggle will be targeted. The political police are not subtle; groups should know if they are targets.

In addition, the FBI and local police may resort to a pen register on a number of phones within the group. A pen register records all phone numbers you dial and, in some cases, all phone numbers of incoming calls to your phone. The phone numbers are systematically attached to names and addresses, and the number of communications between any two numbers is counted. The more frequently two phone numbers are in communication, the more importance is attached to the communications. Nor does this kind of "traffic analysis" stop there. Analyses of most of the important numbers you call reveals still more of a group pattern of interaction by phone. For example, you call person A a great deal, so they analyze person A's traffic. That may reveal that person A calls person X a great deal. Person X's traffic analysis reveals that he or she calls you very frequently. Now they can assume that the three of you constitute a tight-knit sub-group. Further, even the infrequently called numbers may give them invaluable qualitative data.

To frustrate the above is not hard. Use the office and home phone for routine political and personal communication. The political police will undoubtedly learn quite a bit of what goes on, but that cannot be helped. Occasionally, by prearrangement, call a comrade and put false information or a mixture of truth and falsehood into the tapper's ear. The intelligence agency will go crazy trying to find out which is true and which is false. Anything sensitive should not be discussed over the phone directly.

The most important way of frustrating the political police on the phone is to talk in code. The best codes are one-time prearranged codes worked out between the two people. Nicknames are helpful, but they are eventually learned and translated by the political police. Various compromises between group codes and one-time personal codes are usual in even the most sophisticated groups. When extreme caution is necessary, the callers can use a common book to decipher the message. The message would be spoken like this, for example: page 24, paragraph 3, line 9, third word. Or to speed things up: 24, 3, 9, 3 - which would be a single word. The method is clumsy at best, but absolutely safe.

Using a pay phone to call a regular phone number will frustrate the pen register, but not a real tap. It is recommended for calls to people who are unlikely to be targets. Do not use the same pay phone too often or they may tap it. Use a number of pay phones that are not in the same geographical area; intensive surveillance often includes tapping *all* pay phones in an area for a period of time.

Do not call from one pay phone to another. The police now assume that they only reason anyone would make such calls is for a clandestine purpose, and that they would therefore be automatically interested in the contents of such conversations, so they have now programmed their computers to intercept all pay phone-to-pay phone calls.

To cope with the fantastic amount of data recorded, far more than the human agents in the National Security Agency (NSA) could listen to, the NSA has computers that are turned on by code words in your conversation. When a code word is spoken into an NSA recording, the computer alerts the human agents by a special light and singles out that telephone call for NSA analysis. The NSA code words are not hard to guess. For example, we think that any mention of Iran would trip an NSA signal.

Any mention of dope, death, military, etc. would probably trigger a signal. So to avoid alerting NSA to pay phone conversations, you must choose a set of code words that are devoid of importance to NSA. Try nursery rhyme characters, names of paints or colors, names of small towns, etc. Do not use any words with military or spy or organized crime connotations, since NSA's computers will surely be coded for those words. Use only neutral words that have prearranged meanings.

We should re-emphasize that knowing for sure that a phone is tapped invites some sophisticated counter-intelligence operations. In some ordinary conversations, you can not only prearrange to plant false information about your own group, but it is a perfect time to run some operations on the intelligence agencies. For example, a member of the political police is casually spoken about as a source of information. Or a nameless member(s) of the political police is(are) mentioned as the reason so and so got away. Or somebody was paid off for inside information. Or whatever; let your imagination flower! But keep it believable. Within limits, we should be able to do a lot of what they do to us.

Citizenship in Emergency

Can democracy protect us against terrorism?

Elaine Scarry

► For the past year, we have spoken unceasingly about the events of September 11, 2001. But one aspect of that day has not yet been the topic of open discussion: the difficulty we had as a country defending ourselves; as it happened, the only successful defense that day was carried out by the passengers on Flight 93, which crashed in Pennsylvania. The purpose of this essay is to examine that difficulty, and the one success, and ask if they suggest that something in our defense arrangements needs to be changed. Whatever the ultimate answer to that question, we at least need to ask it since defending the country is an obligation we all share.

Speed and Security

The difficulty of defense on September 11 turned in large part on the pace of events. We need to look carefully at the timelines and timetables on that day. But as we do, it is crucial to recall that the word “speed” has been at the center of discussions of national defense for the last fifty years. When we look to any of our literatures on the subject, we find in the foreground statements about the speed of our weapons, of our weapons’ delivery systems, and of the deliberations that will lead to their use.

Throughout this period, the heart of our defense has been a vast missile system, all parts of which are described as going into effect in “a matter of minutes”: a presidential decision must be made in “a matter of minutes”; the presidential order must be transmitted in “a matter of minutes”; the speed of the missile launch must be carried out “in a matter of minutes”; and the missile must reach its target in “a matter of minutes.”

The matter-of-minutes claim is sometimes formally folded into the names of our weapons (as in the Minuteman missile) and other times appears in related banner words such as “supersonic” and “hairtrigger.”¹ Thousands of miles separating countries and continents can be contracted by “supersonic” missiles and planes that carry us there in “a matter of minutes”; and thousands of miles separating countries and continents can be contracted by focusing on the distance that has to be crossed not by the weapon itself but by the hand gesture that initiates the launch—the distance of a hair.

“Speed” has occupied the foreground not only of our *descriptive* statements about our national defense but also our *normative* statements. Our military arrangements for defending the country have often been criticized for moving increasingly outside the citizenry’s control. The constitutional requirement for a Congressional declaration of war has not been used for any war since World War II: the Korean War, the Vietnam War, and the war in former Yugoslavia were all carried out at the direction of the president and without a congressional declaration, as were the invasions of Panama, Grenada, and Haiti.² Speed has repeatedly been invoked to counter ethical, legal, or constitutional objections to the way our weapons policies and arrangements have slipped further and further beyond democratic structures of self-

governance.

This bypassing of the Constitution in the case of conventional wars and invasions has been licensed by the existence of nuclear weapons and by the country's formal doctrine of Presidential First Use, which permits the president, acting alone, to initiate nuclear war.³ Since the president has genocidal injuring power at his personal disposal, obtaining Congress's permission for much lesser acts of injury (as in conventional wars) has often struck presidents as a needless bother.⁴ The most frequent argument used to excuse the setting aside of the Constitution is that the pace of modern life simply does not allow time for obtaining the authorization of Congress, let alone the full citizenry. Our ancestors who designed the Constitution—so the argument goes—simply had no picture of the supersonic speed at which the country's defense would need to take place. So the congressional requirement is an anachronism. With planes and weapons traveling faster than the speed of sound, what sense does it make to have a lot of sentences we have no time to hear?

Among the many revelations that occurred on September 11 was a revelation about our capacity to act quickly. Speed—the realpolitik that has excused the setting aside of the law for fifty years—turns out not to have been very *real* at all. The description that follows looks at the timetables of American Airlines Flight 77—the plane that hit the Pentagon—and United Airlines Flight 93—the plane that crashed in Pennsylvania when passengers successfully disabled the hijackers' mission. Each of the two planes was a small piece of U.S. ground. Their juxtaposition indicates that a form of defense that is external to the ground that needs to be defended does not work as well as a form of defense that is internal to the ground that needs to be protected. This outcome precisely matches the arguments that were made at the time of the writing of the Constitution about why the military had to be “held within a civil frame”: about why military actions, whether offensive or defensive, must be measured against the norms of civilian life, must be brought into contact with the people with whom one farms or performs shared labor, or the people with whom one raises children, or the people with whom one goes to church or a weekly play or movie. Preserving such a civil frame was needed to prevent the infantilization of the country's population by its own leaders, and because it was judged to be the only plausible way actually to defend the home ground.

When the plane that hit the Pentagon and the plane that crashed in Pennsylvania are looked at side by side, they reveal two different conceptions of national defense: one model is authoritarian, centralized, top down; the other, operating in a civil frame, is distributed and egalitarian. Should anything be inferred from the fact that the first form of defense failed and the second succeeded? This outcome obligates us to review our military structures, and to consider the possibility that we need a democratic, not a top-down, form of defense. At the very least, the events of September 11 cast doubt on a key argument that, for the past fifty years, has been used to legitimize an increasingly centralized, authoritarian model of defense—namely the argument from speed.

American Flight 77

American Airlines 77 was originally scheduled to fly from Washington to Los Angeles. The plane approached the Pentagon at a speed of 500 miles per hour.⁵ It entered the outermost of the building's five rings, ring E, then cut through ring D and continued on through ring C, and eventually stopped just short of ring B.⁶ Two million square feet were damaged or destroyed.⁷

Before September 11, the Pentagon was five corridors deep, five stories high, and in its overall shape, five-sided. Three of the Pentagon's five sides were affected (one had to be leveled and rebuilt; the other two were badly damaged by smoke and water).

One hundred and eighty-nine people died—64 on the plane, 125 working in the Pentagon.

Many others were badly burned.⁸ Thousands of people work in the Pentagon.⁹ Two factors prevented many more people from being killed or badly burned. First, the building is stacked horizontally, not vertically like the World Trade Center towers—it is built like layers of sedimentary rock that have been turned on their side and lie flush with the ground. Second, one of the sections hit was being renovated and was therefore relatively empty of people when the plane entered.

While we continue to lament the deaths and injuries, and while we continue to find solace in the fact that the number of deaths and injuries was not higher, one key fact needs to be held on to and stated in a clear sentence: on September 11, the Pentagon could not defend the Pentagon, let alone the rest of the country.

The U.S. military had precious little time to respond on September 11 (and this fact has been accurately acknowledged by almost everyone, both inside and outside the country, who has spoken about the day). But by the standards of speed that have been used to justify setting aside constitutional guarantees for the last fifty years, the U.S. military on September 11 had a luxurious amount of time to protect the Pentagon. They had more than minutes. The pilots of the F-15s and F-16s that flew on September 11 made no mistakes, displayed no inadequacies, and showed no lack of courage—but what they tried to do now appears to have been a structural impossibility.

One hour and twenty-one minutes go by between the moment FAA controllers learn that multiple planes have been taken and the moment the Pentagon is struck. Controllers hear the hijackers on the first seized plane (American Flight 11) say “we have some planes” at 8:24 a.m., a sentence indicating that the plane from which the voice comes is not the sole plane presently imperiled. The information that “some planes” have been taken is available one hour and 21 minutes before the Pentagon is hit by the third seized plane at 9:45 a.m.¹⁰

Fifty-eight minutes go by between the attack on the first World Trade Tower (at 8:47 a.m.) and the crash into the Pentagon (9:45 a.m.). This means that for almost one hour before the Pentagon is hit, the military knows that the hijackers have multiple planes and that those hijackers have no intention to land those planes safely.

The crash of American Flight 77 into the Pentagon comes fifty-five minutes after that plane has now itself disappeared from radio contact (at 8:50 a.m.). So for *fifty-five minutes*, the military now knows three things:

1. the hijackers have multiple planes;
2. the hijackers—far from having any intention of landing the planes safely—intend to injure as many people on the ground as possible;¹¹ and

3. Flight 77 has a *chance* of being one of those planes since it has just disappeared from radio.

When, six minutes later, the plane loses its transponder (so that its radar image as well as its radio contact is now lost), the chance that it is one of the seized planes rises.

By the most liberal reading, then, the country had *one hour and twenty-one minutes* to begin to respond. By the most conservative reading, the country had *fifty-five minutes* to begin to respond.¹² The phrase “begin to respond” does not mean that an F-15 or F-16 could now attack the plane that would hit the Pentagon. At the one hour and twenty-one-minute clock time, the plane that will eventually hit the Pentagon is only four minutes into its flight and has not yet been hijacked. It means instead that a warning threshold has just been crossed and a level of readiness might therefore begin: at one hour and twenty-one minutes, fighter pilots could be placed on standby on the ground with engines running; at fifty-five minutes, fighter planes could be following the third plane, as well as any other planes that are wildly off course with radio contact missing.

One hour and twenty-one minutes and *fifty-five minutes* are each a short time—a short, short time. But . . . by the timetables that we have for decades accepted as descriptive of our military weapons, by the timetables we have accepted as explanations for why we must abridge our structures of self-governance—by the intoxicating timetables of “rapid response,” the proud specifications of eight minutes, twelve minutes, four minutes, one minute—by these timetables, the September 11 time periods of one hour and twenty-one minutes or of fifty-five minutes are very long periods indeed.

The transition from the moment Flight 77’s radio is off (at 8:50 a.m.) to the moment it disappears from secondary radar (8:56 a.m.) is crucial, for it begins to confirm the inference that this is one of the hijacked planes.¹³ A sequence of confirmations now follows. While the FAA controllers have been unable to reach the plane, now the airline company also discovers its inability to reach Flight 77 on a separate radio (shortly after 9 a.m.).¹⁴ At 9:25 a passenger, Barbara Olson, places a phone call to her husband in the U.S. Justice Department, Theodore Olson, stating that the plane is under the control of hijackers.¹⁵ Because the passenger is well known to the Justice Department listener, no time need be lost assessing the honesty and accuracy of the report. This means that twenty minutes prior to the moment the Pentagon is hit, the Justice Department has direct, reliable voice confirmation of the plane’s seizure.

So for *twenty minutes* prior to the hitting of the Pentagon, the military is in the position to know three things (the third of which differs decisively from what it knew at the fifty-five minute marker):

1. the hijackers have multiple planes;
2. the hijackers intend to injure as many people as possible;
3. Flight 77 is *certainly* one of the hijacked planes: it has disappeared from radio, has disappeared from secondary radar, has disappeared from the company radio, and has been described to the Justice Department as “hijacked” by a passenger whose word cannot be doubted.

The steadily mounting *layers of verification* listed in number 3 continue. At 9:33 a.m., an FAA air traffic controller sees on radar a “fast moving blip” (or “fast moving primary target”) making its way toward Washington air space: this level of verification comes *twelve minutes* prior to the plane’s crash into the Pentagon. At 9:36 a.m. an airborne C-130 sees the plane itself and identifies it as a “757 moving low and fast.”¹⁶ This further confirmation comes *nine minutes* prior to the collision. No one can suppose that in nine minutes planes could be scrambled and reach the hijacked plane (even if we have, for decades, listened dutifully to descriptions of much more complicated military acts occurring in nine minutes). But certainly the layers of alert, of scrambling, of takeoff, of tracking, could have begun one hour and twenty minutes earlier, or fifty-five minutes earlier, not nine minutes earlier. Nine minutes is presumably the time frame in which only the last act of military defense need be carried out by the fighter planes—if there is any reasonable last act to be taken, a question to which I will return.

During much of its flight, American Flight 77 was over countryside (rather than over densely populated urban areas).¹⁷ The six successive layers of verification need to be spatially displayed so that we can begin to picture where the plane was during each of them:

- loss of radio (55 minutes remain)
- loss of transponder (49 minutes remain)
- loss of contact with the airline company (approximately 36 minutes remain)
- a passenger calls the Justice Department (20 minutes remain)
- a radar image is seen moving toward Washington whose source is not using its official “secondary” radar (12 minutes remain)
- a C-130 sights a Boeing 757 flying fast and low (9 minutes remain)

Assuming an airspeed of 500 miles an hour, we can infer that at the time we learn that both the radio and the transponder are off (*the second layer of confirmation*), the plane would be 441 miles from Washington with many miles of sparsely populated land beneath it.¹⁸ By *the fourth confirmation* (Barbara Olson’s phone call), it would be 180 miles from Washington. By *the sixth confirmation*, that given by the C-130, the plane destined for the Pentagon would still be 81 miles from Washington and the possibility of minimizing injury to those on the ground would be rapidly vanishing with each passing mile.

Again, the point here is not to say, “Why couldn’t these airmen shoot down the plane?” Time made that extremely difficult. But much smaller units of time have been invoked to explain our battle readiness over the last fifty years and to license the centralization of injuring power rather than a decentralized and distributed authorization across the full citizenry that is, according to the U.S. Constitution, our legal right and our legal responsibility to protect. There is a second profound reason the act could not be (ought not to have been) carried out—the problem of consent, to which I will return when we come to Flight 93.

Let us see what actions the military undertook during this time. The country has fourteen National Guard planes responsible for defending the country. Five of those planes—two F-15s from Otis Air Force Base on Cape Cod and three F-16s from Langley in Virginia—were called into action on September 11. These five planes were not the only military planes in the air that day. Once the Pentagon was hit, the FAA ordered all aircraft to land in a beautifully choreographed landing of 4,546 planes over a period of three hours. When the FAA announced

the order, 206 military planes were in U.S. airspace (most engaged in routine exercises, actions unconnected to the immediate defense of the country); ninety remained in the air after the grounding (their duties have not been entered into the public record).¹⁹ But it is only the five National Guard planes that were called into action against the seized passenger airliners that will be described here.

The two National Guard F-15s that took off from Otis Air Force Base on Cape Cod attempted to address the events taking place in New York City. They were called into action one minute before the first World Trade Center tower was hit; by the time the second tower was hit they were 71 miles—eight minutes—away from Manhattan. Should they then have continued down to the Washington area? (By this time, the plane destined for the Pentagon had its radio and transponder off and was reachable by neither air controllers nor the airline company.) The answer is no. The two F-15s needed to stay near New York City, where it was reasonable to worry that a third hijacked plane could approach. From September 11, 2001, until March 21, 2002, New York airspace was protected 24 hours a day by F-15s, F16s, and AWACS.

Three F-16s at Langley, Virginia, received their first order from Huntress Defense Section at 9:24 a.m. This is a late start: twenty-two minutes after the second World Trade Center tower has been hit, thirty-four minutes after the plane destined for the Pentagon has lost its radio, twenty-eight minutes after it has disappeared from secondary radar, and fifteen minutes after the airline company has failed to reach the plane on its own radio. By 9:30 a.m. the three Langley F-16s are in the air traveling at 600 MPH toward New York City. Soon they are instructed to change their course and are told that Reagan National Airport is the target. They are flying at 25,000 feet.²⁰ The hijacked plane is flying at 7,000 feet. They reach Washington, D.C., at some unspecified time after the 9:45 collision of Flight 77 into the Pentagon. As they pass over the city, they are asked to look down and confirm that the Pentagon is on fire—confirmation that by this point civilians on the ground have already provided.

There are profoundly clear reasons why the military could not easily intercept the plane and bring it down in a rural area. But each of those reasons has counterparts in our longstanding military arrangements that should now be subjected to rigorous questioning. First: Flight 77's path was hard to track since its transponder had been turned off. Yes, that's true—and so, too, any missiles fired on the United States or its allies will surely be traveling without a transponder; their path will not be lucid; their tracking will not be easy. Second, the fact that Flight 77's radio was not working couldn't be taken as a decisive sign that it was a hijacked plane since at least eleven other planes in the country had radios not working (none of the others hijacked). Yes, that's true—and with missile defense there are likely to be not eleven but hundreds of decoys and false targets that will have to be nimbly sorted through. As difficult as it was to identify the third seized plane, it must be acknowledged that the flight had elements that made it far easier to identify than the enemy missiles our nation has spoken blithely about for decades: the direct voice confirmation provided by the passenger phone call to the Justice Department, most notably, will not have any counterpart on a missile attack; nor can we reasonably expect six layers of verification of any one enemy plane or missile.

A third crucial explanation for the failure to protect the Pentagon is that an F-16 cannot shoot down a passenger plane by arrogating to itself the right to decide whether the lives on board can be sacrificed to avert *the possibility* of even more lives being lost on the ground.²¹ Yes, that is true—and yet for decades we have spoken about actions that directly imperil the full

American citizenry (including presidential first use of nuclear weapons against a population that the president acting alone has decided is “the enemy”) without ever obtaining the American citizenry’s consent to those actions.

Each of these three explanations for why the attack on the Pentagon could not be easily averted raises key questions about our longstanding descriptions of the country’s defense, and yet so far does not appear to have in any way altered those descriptions. September 11 has caused the United States and its allies to adjust their timetables only in those cases where the scenario imagined closely approximates the events that occurred in the terrorist attack itself. In England, for example, “MI5 has warned Ministers that a determined terrorist attempt to fly a jet into the Sellafield nuclear plant in Cumbria could not be prevented because it is only *two minutes’* flying time from transatlantic flight paths.”²²

While two minutes’ time makes it impossible to defend Cumbria against terrorists, two minutes is apparently plenty of time for carrying out missile defense by the United States and NATO allies. Here is a post–September 11 description of England’s “Joint Rapid Reaction Force”: “A new satellite communications system has been installed to allow planners in Northwood to transmit target co-ordinates to the royal Navy’s nuclear submarines equipped to fire Tomahawk cruise missiles. HMS *Trafalgar* and HMS *Triumph* in the Indian Ocean both have this system. *Within minutes* of the Prime Minister giving permission to fire from Downing Street, General Reith could pass on the orders to the submarine nominated to launch the precision attack.”²³ What would be the response by Western democracies if a terrorist now used chemical, biological, or even nuclear weapons? In an article describing advice to Tony Blair from his defense ministers, we learn that “one of his most trusted advisers believes that a highly effective way of preventing such an attack is to threaten states that succor the terrorists with a nuclear wipe-out, *within minutes* of such an attack, without waiting for intelligence reports, United Nations resolutions or approval from NATO.”²⁴ Does the Bush administration have plans in place for such attack? Might it be our duty to inquire?

The plane that took the Pentagon by surprise could not be stopped despite a *one hour and twenty-one-minute* warning that multiple planes had been hijacked, despite a *fifty-eight-minute* warning that the hijackers intended to maximize the number of casualties, despite a *fifty-five-minute* warning that Flight 77 might *possibly* be a hijacked flight, and despite a *twenty-minute* warning that Flight 77 was *certainly* a hijacked flight. Yet so confident are we of our ability to get information, of our power to decipher complex lines of responsibility, of the existence of evil and of the transparency of that evil, that we are still today talking about the two or three minutes to send cruise missiles and even nuclear genocide to foreign populations. This despite eleven months—475,000 minutes—in which we have been unable to determine who sent anthrax to the U.S. Senate and various centers of television communication.

United Flight 93

United Airlines Flight 93 was a small piece of American territory—roughly 600 cubic meters in its overall size. It was lost to the country for approximately forty minutes when terrorists seized control. It was restored to the country when civilian passengers who became citizen-soldiers regained control of the ground—in the process losing their own lives.

The passengers on United Flight 93 were able to defend this ground for two reasons: first, they were able to identify the threat accurately because it was in their immediate sensory horizon (unlike the F-16s that hoped to intercept the plane that hit the Pentagon, the passengers on Flight 93 did not need to decipher their plane's flight path from the outside, nor make inferences and guesses about lost radio contact). The passengers were also able to get information from unimpeachable sources external to the plane: crucially, they did not rely on information from a single central authority but obtained it from a distributed array of sources, each independent of the others. Second, it was their own lives they were jeopardizing, their own lives over which they exercised authority and consent. On the twin bases of sentient knowledge and authorization, their collaborative work met the democratic standard of "informed consent."

When the U.S. Constitution was completed it had two provisions for ensuring that decisions about war-making were distributed rather than concentrated. The first was the provision for a congressional declaration of war—an open debate in both the House and the Senate involving what would today be 535 men and women. The second was a major clause of the Bill of Rights—the Second Amendment right to bear arms—which rejected a standing executive army (an army at the personal disposal of president or king) in favor of a militia, a citizen's army distributed across all ages, geography, and social class of men.²⁵ Democracy, it was argued, was impossible without a distributed militia: self-governance was perceived to be logically impossible without self-defense (exactly *what* do you "self-govern" if you have ceded the governing of your own body and life to someone else?)

United Flight 93 was like a small legislative assembly or town meeting. [Figure 2](#) shows the assembly structure. The residents on that ground conferred with one another, as well as with people not residing on the plane. Records from the on-board telephones show that twenty-four phone calls were made between 9:31 a.m. and 9:54 a.m.; additional calls were made from cell phones.²⁶ In approximately *twenty-three minutes*, the passengers were able collectively to move through the following sequence of steps:²⁷

1. *Identify the location throughout the plane of all hijackers and how many people each is holding.* We know that passengers registered this information in detail because they voiced the information to people beyond the plane: Todd Beamer relayed the information to Lisa Jefferson (a Verizon customer-service operator); Jeremy Glick relayed it to his wife;²⁸ Sandy Bradshaw to her husband; Mark Bingham to his mother; Marion Britton to a close friend; Elizabeth Wainio to her stepmother; and CeeCee Lyles to her husband.

In terms of democratic self-defense, these conversations are crucial (both at step one and at each of the seven steps listed below) to preserving the civil frame that the founders identified as so essential to military defense. The conversations enabled extraordinary events to be tested against the norms of everyday life. They were both intimate and an act of record-making: how else to explain Mark Bingham's self-identification to his mother, "This is Mark Bingham." He both gave his mother the statement that the plane had been seized by hijackers ("You believe me, don't you?") and in effect notarized the statement by giving a verbal signature.

2. *Hear from sources outside the plane the story of World Trade Center towers.* This information was key: it informed the passengers that they would almost certainly not be making a safe landing; it also informed them that many people on the ground would also suffer

death or injury from their plane.

3. *Verify by multiple sources outside the plane the World Trade Center story.* Jeremy Glick, for example, told his wife that the account of the World Trade Center attacks was circulating among the passengers. He explicitly asked her to confirm or to deny its truth: “Is it true?”

4. *Consult with each other and with friends outside the plane about the appropriate action.* Jeremy Glick told his family the passengers were developing a plan “to rush” the hijackers and he asked their advice. Todd Beamer told Lisa Jefferson the passengers will “take” the terrorists (she cautioned: “Are you sure that’s what you want to do?”) Tom Burnett told his wife a group of us “is going to do something” (she urged him to lay low and not make himself visible). Sandy Bradshaw told her husband she was at that moment filling coffee pots with boiling water which she planned to throw at the hijackers; she asked if he had a better plan (he tells her she has the best plan and to go ahead).

5. *Take a vote.* Jeremy Glick described the voting process to his wife as it was underway.

6. *Prepare themselves for taking a dire action that may result in death.* CeeCee Lyles, unable to reach her husband, left on the phone a recording of herself praying, then later reached him and prayed with him; Tom Burnett asked his wife to pray while he and others on the plane acted; Todd Beamer and Lisa Jefferson together recited the Twenty-third Psalm.

7. *Take leave of people they love.* Each of the passengers who was in conversation with a family member stated aloud his or her love for the listener; Todd Beamer asked Lisa Jefferson to convey his love to his family. The family members reciprocated: “I’ve got my arms around you,” Elizabeth Wainio’s stepmother told her.

8. *Act.*

Many passengers described the plan to enter the cockpit by force. Not every passenger assumed death was certain. Jeremy Glick left his phone off the hook, telling his wife, “Hold the phone. I’ll be back.” Todd Beamer also left the phone line open—either because he expected to come back, or as an act of public record-keeping. The two open lines permitted members of the Glick household and Lisa Jefferson to overhear the cries and shouts that followed, indicating that action was being taken. CeeCee Lyles, still on the phone with her husband, cried, “They’re doing it! They’re doing it!” Confirmation is also provided by Sandy Bradshaw’s sudden final words to her husband: “Everyone’s running to first class. I’ve got to go. Bye.”²⁹

The passengers on United Flight 93 could act with speed because they resided on the ground that needed to be defended. Equally important, they could make the choice—formalized in their public act of an open vote—between certain doom and uncertain (but possibly more widespread) doom. They could have hoped that the hijackers would change their planned course; they could have known that death by either avenue was certain, but one avenue would take them to their deaths in several minutes (rushing the hijackers and crashing the plane) and the other avenue would perhaps give them another half-hour or hour of life (waiting for the plane to reach its final target). They could have chosen the second; many people have chosen a delayed death when given the same choice. It is, in any event, the right of the people who themselves are going to die to make the decision, not the right of pilots in an F-16 or the person giving orders to the person in the F-16—as both civilian and military leaders have repeatedly

acknowledged since September 11.

It may be worth taking note of the fact that the hijackers themselves correctly foresaw that the threat to their mission would come from the passengers (“citizen soldiers”) and not from a military source external to the plane. The terrorists left behind them multiple copies of a manual, five pages in Arabic.³⁰ The manual is a detailed set of instructions for the hours before and after boarding the plane—“an exacting guide for achieving the unity of body and spirit necessary for success.” The ritualized set of steps includes: taking a mutual pledge to die; carrying out a ritual act of washing, invocation, and prayer; and dressing according to prescribed recommendations on the tightness or looseness of clothing.

The manual does not tell the terrorists what to do if an F-15 or F-16 approaches the planes they have seized.³¹ It instead gives elaborate instruction on what to do if passengers offer resistance. We should not ordinarily let ourselves be schooled by terrorists. But terrorists who seek to carry out a mission successfully have to know what the greatest threat to their mission is—and the handbook indicates that the great obstacle was perceived to be first, the passengers, and second, the reluctance the hijackers might feel to kill any resisting passengers. They are instructed at length and in elaborate detail to kill any resister and to regard the killing as “a sacred drama,” a death carried out to honor their parents. (That the hijackers would unblinkingly crash into a skyscraper taking thousands of lives yet balk at the idea of killing people hand-to-hand and therefore require detailed counseling to get through it is perhaps no more surprising than the fact that we listen every day to casualty rates brought about by the military yet would not keenly kill in hand-to-hand combat.)

Conclusion

I have intended here to open a conversation about our general capacity for self-defense. I have compared the fate of the plane that hit the Pentagon and the plane that crashed in Pennsylvania. The military was unable to thwart the action of Flight 77 despite fifty-five minutes in which clear evidence existed that the plane might be held by terrorists, and despite twenty minutes in which clear evidence existed that the plane was certainly held by terrorists. In the same amount of time—twenty-three minutes—the passengers of Flight 93 were able to gather information, deliberate, vote, and act.³²

September 11 involved a partial failure of defense. If ever a country has been warned that its arrangements for defense are defective, the United States has been warned. Standing quietly by while our leaders build more weapons of mass destruction and bypass more rules and more laws (and more citizens) simply continues the unconstitutional and—as we have recently learned—ineffective direction we have passively tolerated for fifty years. We share a responsibility to deliberate about these questions, as surely as the passengers on Flight 93 shared a responsibility to deliberate about how to act. The failures of our current defense arrangements put an obligation on all of us to review the arrangements we have made for protecting the country. “All of us” means “all of us who reside in the country,” not “all of us who work at the Pentagon” or “all of us who convene when there is a meeting of the Joint Chiefs of Staff.” What the Chiefs of Staff think, or what analysts at the Pentagon think, is of great interest (as are the judgments of men and women who by other avenues of expertise have thoughtful and knowledgeable assessments of security issues); it would be a benefit to the country if such people would now begin to share those views with the public. But such views

can in no way preempt or abridge our own obligation to review matters, since the protection of the country falls to everyone whose country it is.

More particularly, September 11 called into question a key argument that has been used to legitimate the gradual shift from an egalitarian, all-citizens' military to one that is external to— independent of—civilian control: the argument from speed. The egalitarian model turned out to have the advantage of swiftness, as well as obvious ethical advantages. This outcome has implications for three spheres of defense.

1. *Defense against aerial terrorism.* To date, the egalitarian model of defense is the only one that has worked against aerial terrorism. It worked on September 11 when passengers brought down the plane in Pennsylvania. It again worked on December 22, 2001, when passengers and crew on an American Airlines flight from Paris to Miami prevented a terrorist (now called “the shoe bomber”) from blowing up the plane with plastic explosives and killing 197 people on board. Two Air Force F-15s escorted the plane to Boston and, once the plane landed, FBI officials hurried aboard; but the danger itself was averted not by the fighter jets or the FBI but by men and women inside the plane who restrained the 6'4" man using his own hair, leather belts, earphone wires, and sedatives injected by two physicians on board.

When a passenger plane is seized by a terrorist, defense from *the outside* (by a fighter jet, for example) appears to be structurally implausible from the perspective of time, and structurally impossible from the perspective of consent. The problem of time—time to identify that a plane has been seized, time to identify accurately which plane it is, time to arrive in the airspace near the seized plane—was dramatically visible in the case of the plane that hit the Pentagon, even though much more time and more layers of verification were available that day than are likely to be available in any future instance. The time difficulty was visible again on January 5, 2002, when a fifteen-year-old boy took off without authorization from Petersburg-Clearwater International Airport, crossed through the airspace of MacDill Air Force Base (the headquarters for the U.S. war in Afghanistan), and then flew into a forty-two-story Bank of America skyscraper in Tampa, hitting at the twenty-eighth floor. Two F-15 fighter jets “screamed” toward him from the south, but reached him only after he had completed his twenty-five minute flight.³³ The time problem was visible once more on June 19, 2002, when a pilot and passenger in a Cessna 182 accidentally crossed into forbidden Washington Monument airspace, flew there for twelve miles (coming within four miles of the White House), and then crossed out again before armed F-16s from Andrews Air Force Base could reach them.

Even if the nearly insurmountable problems of time and perfect knowledge can one day be solved, how can the problem of consent be solved? There is no case in war where a soldier is authorized to kill 200 fellow soldiers; how can an airman be authorized to kill 200 fellow citizens? How can anyone other than the passengers themselves take their lives in order to save some number of the rest of us on the ground? During the seven months that F-15s and F-16s, armed with air-to-air missiles, flew round the clock over New York and Washington, what instructions did they have in the event that a passenger plane was seized? What instructions do they now have for their more intermittent flights? Are such instructions something only high-ranking officials should be privy to, or might this be something that should be candidly discussed in public?

It seems reasonable to conclude that on September 11 the Pentagon could have been defended

in one way and one way only, by the passengers on the American Airlines flight. This would have required three steps: that multiple passengers on the plane be informed about the World Trade Center towers;³⁴ that the passengers decide to act or instead to abstain from acting; and that, in the event that they choose to act, they be numerous enough to successfully carry out their plan. As far as we know, none of these steps took place—in part because, as far as we know, there were not multiple passengers on board who knew about the World Trade Center towers. It is possible that one or more of these steps took place, even though they have not been recorded.

In stating that the egalitarian model is our best and only defense against aerial terrorism, I do not mean that passengers in any one case *must* choose to act, or that—having so chosen—they will be successful. I mean only that this is the one form of defense available to us as a country, which passengers are at liberty to exercise or refrain from exercising. Measures taken by the nation that are internal to the plane (locks on cockpit door, the presence of air marshals, the cessation of the round-the-clock fighter jets over New York and Washington³⁵) are compatible with this form of defense.

2. National defense in the immediate present. The contrast between the plane that hit the Pentagon and the plane that crashed in Pennsylvania invites consideration of the need to return to an egalitarian and democratic military not only in the specific case of aerial terrorism but in all measures we take for the nation's defense in the present year. Some may argue that we cannot generalize from one day. Can we generalize from zero days? One day is what we have. What makes this non-risky is that rather than requiring us to come up with some new system of government, all it requires is returning to, and honoring, the framework of our own laws.

Since September 11 we have witnessed many actions taken in the name of homeland defense that are independent of, or external to, civilian control. Foreign residents have been seized and placed in circumstances that violate our most basic laws; the war against Afghanistan was underway before we had even been given much explanation of its connection to the terrorists, who were all from Saudi Arabia or Lebanon or Egypt or the United Arab Emirates and not from Afghanistan; that war now seems to be over even though we don't know whether we eliminated the small circle around Osama bin Laden, for whose sake we believed we were there; we are now tripping rapidly ahead to the next war, listening passively to weekly announcements about an approaching war with Iraq that has no visible connection to the events of September 11; the president's formulation of this future war sometimes seems to include (or at least not to exclude) the use of nuclear weapons and the animation of our nuclear first-use policy.³⁶ The decoupling of all defense from the population itself lurches between large outcomes (presidential declaration of war) and the texture of everyday life. According to the former chairman of the Federal Communications Commission, the federal agency called the National Communications Systems has "proposed that government officials be able to take over the wireless networks used by cellular telephones in the event of an emergency," thereby pre-empting the very form of defense that did work (the citizenry) and giving their tools to the form of defense that did not work (the official government).³⁷

We are defending the country by ceding our own powers of self-defense to a set of managers external to ourselves. But can these powers be ceded without relinquishing the very destination toward which we were traveling together, as surely as if our ship had been seized? The

destination for which we purchased tickets was a country where no one was arrested without their names being made public, a country that did not carry out wars without the authorization of Congress (and the widespread debate among the population that such a congressional declaration necessitates), a country that does not threaten to use weapons of mass destruction. Why are we sitting quietly in our seats?

In the short run, returning to an egalitarian model of defense means: no war with Iraq unless it has been authorized by Congress and the citizenry; no abridgment of civil liberties; no elimination of the tools that enable citizens to protect themselves and one another (such as cell phones)—and above all, no contemplated use of nuclear weapons.

3. *National defense in the long run.* Europeans often refer to nuclear weapons as “monarchic weapons” precisely because they are wholly external to any powers of consent or dissent exercised by the population. In the long run, the return to an egalitarian model of national defense will require the return to a military that uses only conventional weapons. This will involve a tremendous cost: it will almost certainly, for example, mean the return of a draft. But a draft means that a president cannot carry out a war without going through the citizenry, and going through the citizenry means that the arguments for going to war get tested tens of thousands of times before the killing starts.

Our nuclear weapons are the largest arsenal of genocidal weapons anywhere on earth. These weapons, even when not in use, deliver a death blow to our democracy.³⁸ But even if we are willing to give up democracy to keep ourselves safe, on what basis have we come to believe that they keep us safe? Their speed? A Cessna plane (of the kind that proved impossible to intercept in Florida and Washington) travels at approximately 136 feet per second; a Boeing 757 (of the kind that proved impossible to intercept as it approached the Pentagon) travels at 684 feet per second; a missile travels at 6,400 feet per second.³⁹ On what have we based our confidence about intercepting incoming missiles, since the problem of deciphering information and decoupling it from false decoys will (along with speed) be much higher in the case of the missile than in the cases of the planes?⁴⁰

Nuclear weapons are an extreme form of aerial terrorism. It is with good reason that we have worked to prevent the proliferation throughout the world of nuclear weapons (as well as biological and chemical weapons of mass destruction). But in the long run other countries of the world will only agree to abstain from acquiring them, or to give them up in cases where they already have them, when and if the United States agrees to give them up. The process of persuading Iraq, China, North Korea, India, Pakistan, as well as our immediate allies, to give them up will commence on the day we agree to restore within our own country a democratic form of self-defense. ■

Elaine Scarry is Walter M. Cabot Professor of aesthetics and the general theory of value, is author of many books, including *The Body in Pain*, *On Beauty*, and *Dreaming by the Book*.

Notes

1. As with the matter-of-minutes vocabulary, the hairtrigger description is widely understood to apply either to the material act of firing a weapon or the mental act of deliberating. In the

spring of 2001, Peace Links asked U.S. President Clinton and Russian President Putin to take all weapons off “*hair-trigger status*,” which gives “both countries *three minutes* to decide whether to launch nuclear missiles once the military tells them it thinks they have spotted an incoming missile.” *South Bend Tribune*, 29 April 2001. Italics added.

2. On the question of whether the country had a constitutional declaration of war against Iraq in the Gulf War, see Michael J. Glennon, “The Gulf War and the Constitution,” *Foreign Affairs* 70 (Spring 1991): 84–101.

3. Presidential First Use of Nuclear Weapons became a formal written policy in “Presidential Directive 59” during the Carter Administration; it has been the country’s official policy during the entire nuclear age. On Eisenhower’s deliberations, for example, about using a nuclear weapon in the Taiwan Straits (1954) and again in Berlin (1959), see E. Scarry, “The Declaration of War: Constitutional and Unconstitutional Violence,” in Austin Sarat and Thomas Kearns, eds., *Law’s Violence*, Amherst Series in Law, Jurisprudence, and Social Thought (Univ. of Michigan Press, 1992), 23–77.

4. For example, President Bush Senior boasted, “I didn’t have to get permission from some old goat in the United States Congress to kick [Iraqi President] Saddam Hussein out of Kuwait” (*Washington Post*, 21 June 1992, A18).

5. On the speed of Flight 77, see note 18 below.

6. “United States Department of Defense News Briefing,” *M2 Presswire* for 17 September 2001 states that it broke through the wall of corridor C, penetrating into the driveway that separates ring C from ring B (but it does not cite any damage to the B ring).

7. Angie Cannon, “The ‘Other’ Tragedy,” (*U.S. News and World Report*, 131:24 10 December 2001), 22.

8. ABC News, Sept. 14, 2001, described both the terrible burn injuries and the “wind of fire” spreading through the building. Angie Cannon in “The ‘Other’ Tragedy” gives an extended account of the injuries. Because no planes could fly into Washington, medical centers from around the country enlisted the help of marathon drivers to carry replacement skin: two drivers from Texas, according to Cannon, drove 70 square feet of skin to Washington in 23 hours and 12 minutes, stopping only for drive-through sandwiches and bathroom breaks; 30 square feet of skin arrived from Cincinnati in 12 hours; two surgeons at Washington Hospital Center, Dr. Jordan and Dr. James Jeng, “worked 12– to 16–hour days” for three weeks.

9. The figure of 23,000 is given on the Pentagon website.

10. Three different times have been given for the crash of Flight 77 into the Pentagon: 9:38 a.m., 9:41 a.m., and 9:45 a.m. I cite the 9:45 a.m. time because it is given by many different reporters, both as a designation of the minute the plane “pierced” the Pentagon and as the minute interviewed eyewitnesses observed the impact, beginning on September 11 and 12 (CNN broadcasts throughout the afternoon of September 11, *Facts on File* for September 11, 2001, September 12 articles in the *New York Times*, *Newsday*, *Chicago Tribune*, *Atlanta Journal and Constitution*, *International Herald Tribune*, *Baltimore Sun*). In the weeks and months that followed, 9:45 a.m. continued to be used in multiple reports both within any

single journal (*New York Times*, September 13, 15, 16 and November 4, 2001) and across many different journals (for example, *New Yorker*, September 23; *Boston Globe*, November 23; *CNN Live*, December 15, 2001. The early time designation of 9:38 a.m. has been introduced into the picture by the Pentagon (at first using the figure of 9:37 a.m.). On September 19, *Facts on File* noted: “the Defense Department placed [the crash] at 9:37 a.m. despite previous reports of 9:45 a.m.”; and on the same day, the *New York Times* described 9:37 a.m. as the time “when the Pentagon estimates that the third hijacked jet crashed into the Pentagon.” The Pentagon has had a series of commemorations, each beginning at 9:38 a.m. (starting with the three-month ceremony on December 11) and reporters have used this time in covering those events. But as the September through December publication dates listed above indicate, many journals and broadcasts have continued to use the 9:45 a.m. minute in describing the crash of the plane itself.

11. Presumably only the first of the two World Trade Center collisions was needed for the nation to know this second piece of information, that the seized planes would not land safely. But if one wants to base this knowledge on the destruction of both World Trade Center towers (hit at 8:47 a.m. and 9:02 a.m.), then the nation had 43 minutes in which it knew that multiple planes were involved, that Flight 77 was likely to be one of the planes (since it had disappeared from radar even before the second tower was hit), and that no safe landing was likely.

12. Using the collision time of 9:38 a.m. (rather than 9:45 a.m.), the two periods would be *one hour and thirteen minutes* and *forty-eight minutes*.

13. The times for the loss of radio and transponder are included in Glen Johnson’s in-depth account, “Probe Reconstructs Horror,” *Boston Globe*, 23 November 2001, 44–45.

14. At this point, American Airlines lacks any clear idea of the plane’s location. At 9:09 a.m., American Airlines thinks Flight 77 may have gone into second World Trade Center tower.

15. Barbara Olson also places a second call to the Justice Department several minutes later.

16. The timetable for both the air controllers’ and pilots’ sightings are given in Matthew L. Wald and Kevin Sack, “A Nation Challenged: The Tapes,” *New York Times*, 16 October 2001, 1.

17. The exact flight path must by now have been precisely reconstructed, but it does not yet appear to be part of the public record. In any event, we know that the plane did not steadily circle Washington, D.C., or any other densely populated spot.

18. These mileage estimates are based on the supposition that Flight 77 was flying at the same 500-mph speed at which World Trade Center planes were flying as they moved down the Hudson Valley at twice the legal airspeed. Both air traffic controllers and the C-130 pilots described Flight 77 as “fast moving.” (The *New York Times*, 16 October 2001, states that Flight 77 was moving at 500 mph when it hit the Pentagon. *U.S. News and World Report*, 10 December 2001, says the impact took place at a speed of 350 MPH).

19. See David Bond’s detailed account in “Crisis at Herndon: 11 Airplanes Astray,” *Aviation Week and Space Technology*, 17 December 2001, 96ff.

20. *New York Times*, 16 October 2001.

21. A retired official of the F.A.A. said, several days after the event, “There is no category of ‘enemy airliners’” and added that he could recall no incident in which a military plane had ever fired on a civilian plane. Matthew L. Wald, “After the Attacks: Sky Rules,” *New York Times*, 15 September 2001, 1. Major General Mike J. Haugen said that the crash of United Flight 93 initiated by the passengers “kept us from having to do the unthinkable . . . and that is to use your own weapons and own training against your own citizens” (*New York Times*, 16 October 2001).

22. Peter Beaumont, “Bin Laden in Plot to Bomb City: Terror Blueprint for Attack on London,” *The Observer*, 16 December 2001, 1. Italics added.

23. Tim Ripley, “Global Army Controlled from a Suburban Bunker,” *The Scotsman*, 2 October 2001, 6. Italics added.

24. Chris Buckland, “Meeting Hell with Horror,” *News of the World*, 30 September 2001. Italics added.

25. For full analyses of the distributive intention of the right to bear arms see Elaine Scarry, “War and the Social Contract: Nuclear Policy, Distribution, and the Right to Bear Arms,” *University of Pennsylvania Law Review* 139 (May 1991): 1257–1316; and Akhil Reed Amar, *The Bill of Rights* (Yale Univ. Press, 1998), 46–63.

26. Most of the narrative details of Flight 93 that follow here as well as in figure 2 come from two sources: “Forty Lives, One Destiny: Fighting Back in the Face of Terror,” *Pittsburgh Post-Gazette*, 28 October 2001, a 6,000-word study; and “Final Words from Flight 93,” *U.S. News and World Report* 131:18 (29 October 2001), 32f, a story coauthored by Angie Cannon, Janet Rae-Dupree, Suzie Larsen, and Cynthia Salter. The passenger and crew quotations provided in these two in-depth news stories recur (with small variations) in Jere Longman, *Among the Heroes: United Flight 93 and the Passengers and Crew Who Fought Back* (HarperCollins, 2002), a book which became available after the writing of this article was complete. It contains richly textured portraits of the 37 passengers and seven crew (both their backgrounds and their actions on September 11). Although the book’s purpose is to celebrate the passengers and crew of Flight 93, rather than to raise questions about U.S. defense, the preface notes that “they accomplished what security guards and military pilots and government officials could not” (x).

27. The overall time frame, from the moment the passengers first expressed their knowledge of the seizure at 9:31 a.m. to the moment the plane was on the ground at 10:10 a.m., is thirty-nine minutes: the reader may therefore wish to assess the sequence of steps in terms of thirty-nine rather than twenty-three minutes. I have used the twenty-three-minute frame because we only have information up through the moment the passengers collectively decided to act, not during the moments when control of the plane was wrestled over or during the time the plane fell toward the ground (the transcript of the voice recorder from the plane that would provide information about this period has so far been withheld from the public by the FBI).

28. In Jeremy Glick’s case, family members used a second phone to contact the New York State Police, who then “patched in” to Jeremy Glick’s phone call and listened to the ongoing

descriptions of the hijacking he was giving.

29. The withholding of the plane's voice tape from the public has permitted rumors to exist that the military shot the plane down (despite consistent government statements that the military took no action). The open passenger phone lines verify that quite apart from whatever the military did or did not do, the passengers themselves did act. The fact that government officials who have heard the plane's voice tape (most notably President Bush) have publicly celebrated the courage of the passengers reinforces what the public phone lines themselves already make clear.

30. Kanan Makiya and Hassan Mneimneh, translators and interpreters, "Manual for a 'Raid'," in *New York Review of Books*, 17 January 2002, 18.

31. Perhaps more accurately, they are told that such matters are beyond their own agency: "All [the United States'] . . . equipment and all their gates and all their technology do not do benefit or harm except with the permission of God." In contrast, harm from resistant passengers is not left to God but is something the manual requires the hijackers to address.

32. They left a wide margin of safety: many miles of terrain still stood between the plane and whatever target in Washington or New York was the terrorists' destination.

33. A Coast Guard plane, already in the air, got close enough to instruct him by hand signals to land, but the boy declined to follow these instructions. See Brad Smith, "Skyscraper Hit," *Tampa Tribune*, 6 January 2002, 1.

34. The events on the Pennsylvania plane clearly depended on the two-directional exchange of information between passengers and friends on the ground. There is probably a useful generalization that can be made here. Communication on planes between passengers and people on the ground should be made as easy as possible, since the most likely way passengers will get crucial information in an emergency is by being able to speak with friends or family. Emergency telephone links between passengers and government officials (FBI, FAA, Air Force, Pentagon) are much less likely to be helpful because in our present era government officials do not believe in two-directional exchanges of information with citizens.

35. Congressional testimony explaining the cessation of round-the-clock flights (Operation Noble Eagle) focused on the expense in dollars (\$50 million a week), in use of airmen (11,000 airmen in comparison with 14,000 airmen for the war in Afghanistan, according to the *New York Times*, 18 March 2002), and in wear and tear on the planes, rather than on the futility of this form of defense. However, the Air Force chief of staff testified to the Senate Armed Services Committee that air marshals inside the planes themselves were a more efficient solution than the fighter jets (Gen. John P. Jumper, March 7, 2002, Senate Armed Services Committee hearing). Because Gen. Jumper was told by Senator Warner that he should give his assessment of the combat air patrols twice—first in a nonclassified and then in a classified form—we do not know his full thoughts on the matter.

36. For example, President Bush's June 1, 2002, graduation speech at West Point had three features which together seemed to make it an announcement (however blurry and genial) of the possibility of a nuclear first strike: it stressed preemptive action; it left the form of preemption (ground invasion, air strike) unspecified; and it explicitly summoned nuclear

weapons, rejecting as inadequate and “too late” the Cold War strategy of “massive retaliation.” Transcript, Federal News Service, June 1, 2002. Although immediate news coverage did not mention the word “nuclear,” the phrases “first strike” and “preemptive first strike” were widely used in the United States (on ABC News, for example, where Sam Donaldson asked, “When do we take these other nations out?”) and internationally (headlines for the *London Daily Telegraph*, *The Guardian*, *The Independent*, and *The Herald* of Glasgow all described President Bush as warning of a “first strike,” and the *Financial Times* emphasized “pre-emptive, unilateral action”).

37. Reed Hundt, “A Better Network for Emergency Communications,” *New York Times*, 25 December 2001. Discussions of phone use during emergencies often pose the choice of whether we want citizens or instead firemen to have phone access. But during the days following September 11, there were many reports of both citizens and firemen having difficulty completing calls. According to an article in *Government Executive* (October 2001), government executives (including financial leaders, federal executives, utility managers, and relief workers) had a 95 percent success rate in making calls during this period because they are beneficiaries of Government Emergency Telecommunication Service (GETS), which gives their calls priority over ordinary users of “AT&T, Spring, and WorldCom.”

38. For discussion of the democratic structures violated by nuclear weapons see Elaine Scarry, “War and the Social Contract” and “Declaration of War.” (See notes 3 and 25.)

39. See Paul Bracken, *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (HarperCollins, 1999), 64.

40. On the decoy problem, see Stephen Weinberg, “Can Missile Defense Work,” *New York Review of Books*, 14 February 2002: “The big problem, as it has been since the days of Nike X, is that any number of interceptor missiles could be used up in attacking decoys that had been sent by the attacker along with its warheads” (42); and Ted Postol, “What’s Wrong With Missile Defense?” *Boston Review* 26:5 (October/November 2001), 40–45.

Originally published in the [October/November 2002](#) issue of *Boston Review*

thousands who were victims of Pinochet's reign of terror. In 1975, she and her mother were imprisoned and tortured in Villa Grimaldi, known for its wooden isolation cubicles, so small that prisoners could only crouch. Her father, a military officer, had refused to go along with the coup and was murdered by Pinochet's men.

In December 2006, a month after Friedman's death, Latin America's leaders gathered for a historic summit in Bolivia, held in the city of Cochabamba, where a popular uprising against water privatization had forced Bechtel out of the country several years earlier. Morales began the proceedings with a vow to close "the open veins of Latin America."²⁵ It was a reference to Eduardo Galeano's book *Open Veins of Latin America: Five Centuries of the Pillage of a Continent*, a lyrical accounting of the violent plunder that had turned a rich continent into a poor one. The book was first published in 1971, two years before Allende was overthrown for daring to try to close those open veins by nationalizing his country's copper mines. That event ushered in a new era of furious pillage, during which the structures built by the continent's developmentalist movements were sacked, stripped and sold off.

Today Latin Americans are picking up the project that was so brutally interrupted all those years ago. Many of the policies cropping up are familiar: nationalization of key sectors of the economy, land reform, major new investments in education, literacy and health care. These are not revolutionary ideas, but in their unapologetic vision of a government that helps reach for equality, they are certainly a rebuke to Friedman's 1975 assertion to Pinochet that "the major error, in my opinion, was . . . to believe that it is possible to do good with other people's money."

Though clearly drawing on a long militant history, Latin America's contemporary movements are not direct replicas of their predecessors. Of all the differences, the most striking is an acute awareness of the need for protection from the shocks of the past—the coups, the foreign shock therapists, the U.S.-trained torturers, as well as the debt shocks and currency collapses of the eighties and nineties. Latin America's mass movements, which have powered the wave of election victories for left-wing candidates, are learning how to build shock absorbers into their organizing models. They are, for example, less centralized than in the sixties, making it harder to demobilize whole movements by eliminating a few leaders. Despite the overwhelming cult of personality surrounding Chávez, and his moves to centralize power at

the state level, the progressive networks in Venezuela are at the same time highly decentralized, with power dispersed at the grass roots and community level, through thousands of neighborhood councils and co-ops. In Bolivia, the indigenous people's movements that put Morales in office function similarly and have made it clear that Morales does not have their unconditional support: the barrios will back him as long as he stays true to his democratic mandate, and not a moment longer. This kind of network approach is what allowed Chávez to survive the 2002 coup attempt: when their revolution was threatened, his supporters poured down from the shantytowns surrounding Caracas to demand his reinstatement, a kind of popular mobilization that did not happen during the coups of the seventies.

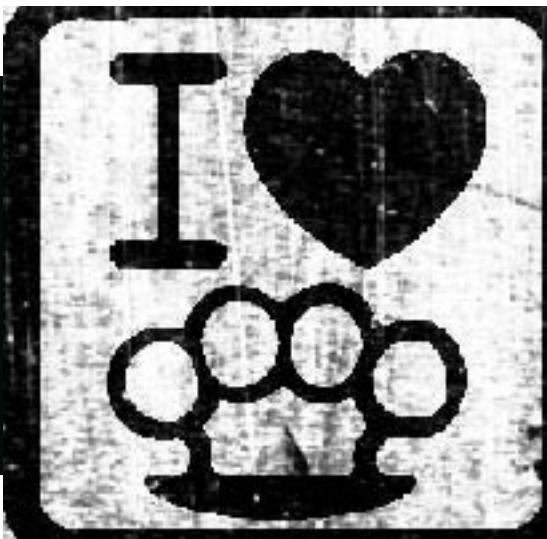
Latin America's new leaders are also taking bold measures to block any future U.S.-backed coups that could attempt to undermine their democratic victories. The governments of Venezuela, Costa Rica, Argentina and Uruguay have all announced that they will no longer send students to the School of the Americas (now called the Western Hemisphere Institute for Security Cooperation)—the infamous police and military training center in Fort Benning, Georgia, where so many of the continent's notorious killers learned the latest in "counterterrorism" techniques, then promptly directed them against farmers in El Salvador and auto workers in Argentina.²⁶ Bolivia looks set to cut its ties with the school, as does Ecuador. Chávez has let it be known that if an extremist right-wing element in Bolivia's Santa Cruz province makes good on its threats against the government of Evo Morales, Venezuelan troops will help defend Bolivia's democracy. Rafael Correa is set to take the most radical step of all. The Ecuadorean port city of Manta currently hosts the largest U.S. military base in South America, which serves as a staging area for the "war on drugs," largely fought in Colombia. Correa's government has announced that when the agreement for the base expires in 2009, it will not be renewed. "Ecuador is a sovereign nation," said the minister of foreign relations, María Fernanda Espinosa. "We do not need any foreign troops in our country."²⁷ If the U.S. military does not have bases or training programs, its power to inflict shocks will be greatly eroded.

The new leaders in Latin America are also becoming better prepared for the kinds of shocks inflicted by volatile markets. One of the most destabilizing forces of recent decades has been the speed with which capital can pick up and move, or how a sudden drop in commodity prices can devastate an entire agricultural sector. But in much of Latin America these shocks have already happened, leaving behind ghostly industrial suburbs and huge

stretches of fallow farmland. The task of the region's new left, therefore, has become a matter of taking the detritus of globalization and putting it back to work. In Brazil, the phenomenon is best seen in the million and a half farmers of the Landless Peoples Movement (MST) who have formed hundreds of cooperatives to reclaim unused land. In Argentina, it is clearest in the movement of "recovered companies," two hundred bankrupt businesses that have been resuscitated by their workers, who have turned them into democratically run cooperatives. For the cooperatives, there is no fear of facing an economic shock of investors leaving, because the investors have already left. In a way, the reclamation experiments are a new kind of post-disaster reconstruction—reconstruction from the slow-motion disaster of neoliberalism. In sharp contrast to the model offered by the disaster capitalism complex in Iraq, Afghanistan and the Gulf Coast, the leaders of Latin America's rebuilding efforts are the people most affected by the devastation. And unsurprisingly, their spontaneous solutions look very much like the real third way that had been so effectively shocked out of the way by the Chicago School campaign around the world—democracy in daily life.

In Venezuela, Chávez has made the co-ops a top political priority, giving them first refusal on government contracts and offering them economic incentives to trade with one another. By 2006, there were roughly 100,000 cooperatives in the country, employing more than 700,000 workers.²⁸ Many are pieces of state infrastructure—toll booths, highway maintenance, health clinics—handed over to the communities to run. It's a reverse of the logic of government outsourcing—rather than auctioning off pieces of the state to large corporations and losing democratic control, the people who use the resources are given the power to manage them, creating, at least in theory, both jobs and more responsive public services. Chávez's many critics have derided these initiatives as handouts and unfair subsidies, of course. Yet in an era when Halliburton treats the U.S. government as its personal ATM for six years, withdraws upward of \$20 billion in Iraq contracts alone, refuses to hire local workers either on the Gulf Coast or in Iraq, then expresses its gratitude to U.S. taxpayers by moving its corporate headquarters to Dubai (with all the attendant tax and legal benefits), Chávez's direct subsidies to regular people look significantly less radical.

Latin America's most significant protection from future shocks (and therefore from the shock doctrine) flows from the continent's emerging independence from Washington's financial institutions, the result of greater integration



confronting snitch culture:

historical examples and current proposals

"Homeboy was talking to the po-po, we had to let everybody that was a no-no, he thought he was on the low low, and was surprised when I hit him with the fou(4)-fou(4)"

-Uncle Murda, "Bullet, Bullet"

With the growing wave of repression by the state towards direct action oriented struggles, radicals have been bombarded with the shameful concern of snitches and informants. In a struggle which is purely of choice and individual realization, as opposed to a rich cultural or family heritage, a valor dedication to one's community has been shamefully neglected by some. The following article provides a brief look into how radical communities of the past have approached traitors to the community, while at the same time proposing how more unique struggles can learn from it. It is an excerpt from the zine; "Got the Hallow Points for the Snitches".

To order a copy of this pamphlet, you can contact the email below:
thegreenscare@gmail.com

As Anarchists, we fight in the face of what appears to be insurmountable odds; our project of liberation is the natural enemy of the culture of authority and capitalism we now live under. Considering that our revolt against the institutions of domination are not isolated pockets of resistance, and that we do not live separately from the rest of society, our communities are inevitably affected --and perhaps infected-- by the culture we are aiming to destroy.

Snitch Culture is not exclusive to Communities in Resistance, but is one thread of control in the larger social fabric of America. Those in power want people to snitch on each other-- especially those from communities that are targeted in particular by the government and are therefore more vulnerable to Snitch Culture-- because snitching works to create a climate of fear and mistrust that can fragment the populations that threaten the structures of power.

For example, in the war against the poor and people of color --those that fill the prisons of America-- the State promotes snitching as a means to perpetuate crime by creating a 'revolving door' in which low-level drug dealers, addicts, and other petty offenders are arrested and released with orders to provide more information in order to create more arrests in order to fill more prisons. The effects of this cycle of snitch-and-prison are that entire communities are torn apart, families broken up, and the United States has the largest prison population in the world.

In Anarchist circles everyone knows that Snitch Culture breaks solidarity among activists and paralyzes our ability to wage effective resistance. Though there is much complaining and hand-wringing about the divisive role snitches play in our communities, we have engaged in very little constructive action about this serious and persistent problem. This zine is an attempt to educate and foster dialogue in our communities in order to develop effective strategies for dealing with snitches and to forge a resistance that can withstand the attacks of power.

To start, we must realize that Snitch Culture is not a new phenomena or only particular to Anarchists, and that many Communities of Resistance in North America and Europe have come up with a number of different ways --some more effective than others-- to deal with Snitch Culture while maintaining their core values.

There are three components --perhaps of unequal importance-- that resistance groups and others have traditionally used to determine their response to snitches: practicality, the agreeability to the core values of the group, and tactical benefit.

The ultra-militant Red Army Faction (RAF) in West Germany tried to use something called "Revolutionary Discipline" to respond to a growing number of snitches. This discipline drew heavily on the promise of immediate personal reprisals for snitching. Snitches both in jail and out were subject to vicious beatings and in one case, a snitch was blinded. This type of response was practical for the RAF because they had a number of supporters both inside and outside of jail. Most snitches could be easily located and jumped by supporters or actual RAF members. It was agreeable to the RAF because it fit in with their concepts of both Revolutionary Discipline and a glorification of violence. However, it did not prove to be an effective tactic for reducing the impact of snitches. By the end of the RAF's existence, snitches were an important part of the State's efforts to not only disrupt, but to arrest numerous members of the RAF-- including its leadership.

The tactics they employed did not seem to reduce Snitch Culture within their own ranks or of other contemporary militant radical organizations in West Germany.

The Weather Underground (WU) also had an extreme but somewhat different strategy when confronting the problem of snitches. The WU used terror as a way to stop the effectiveness of snitches. They required all members to give the names and addresses of close friends and family and were explicitly warned --sometimes while on psychedelic drugs-- that if they snitched, they and their family would be subject to violent reprisals. In one rambling message from the WU --written after an AIM snitch took the stand against former comrades-- published in radical periodicals at the time and believed to have been written by Bernadine Dorn, stated that the WU was not afraid to support the "[Charlie] Manson approach" when it came to "bringing hell on Earth for pig-snitches." It went into detail about how violently the WU would deal with snitches and their friends and family. This approach ended up being completely impractical for the WU because they had neither the members nor the support to pull off such grandiose plans. By the nature of being underground, they were marginalized and had little ability to strike out at snitches in any way. In fact, there is no evidence that any snitch on the WU was ever even bothered by the group. Whether this approach of terror was agreeable to the core values of the WU is hard to say since the WU position on violence and acceptable violence seemed to change constantly. It was however, consistent with the ultra-violent streak in the core leadership of the group. As a tactic it was counter-productive-- it caused considerable debate in radical circles and most of it was negative. The cops also had little trouble turning folks associated with the WU, and a number of the most rhetorically violent members of the leadership either turned themselves in, or cut deals.

No resistance group in recent times can compare to the Black Panther Party (BPP) --and its factions-- in terms of being completely infiltrated by snitches as well as law enforcement! The BPP, in the popular mind, is associated with violence and ultra-militancy. The image of a tough leather-clad Black Panther carrying a shotgun is an ever present part of the iconography of the radical left. One would think that the BPP's approach to snitches would be similar to the RAF and the WU; however, they took a completely different approach and relied on community shame as a mechanism for dealing with snitches. This was a somewhat practical approach because they had a number of widely circulating publications and outlets to get information about snitches out. They also were followed closely by the radical left and had access to a staggering number of mediums to report to the broader cultures of resistance. It was certainly agreeable to the ideals of the BPP, which claimed to be the voice of specific communities and saw itself as a community-based organization. Tactically, the record speaks for itself. There were a large number of snitches, many who were not named until well after the fall of the BPP, and the government --which was particularly brutal and repressive in dealing with the BPP-- never had trouble turning members affiliated with the BPP against the organization. In Chicago, for example, the number of

snitches was nearly epidemic.

While the above examples are not particularly positive, they illustrate some of the difficulties we face in dealing with snitches today in our own communities --and thus the need for dialogue. However, groups like the Irish Republican Army (IRA), the Basque Separatists (ETA), and namely the WWII French Resistance Fighters (The Maquis), are positive examples of Communities in Resistance that dealt successfully with Snitch Culture. The Maquis, according to Gestapo/Vichy records, show that less than 5% of all detainees were "cooperative". William Volman, in his book, *Rising Up and Rising Down*, says that the Spanish --and French-- governments have "never been successful in creating a culture of informants". The key is to learn from the mistakes of the past and forge our own response to snitches that is practical, agreeable to our core values, and tactically beneficial.

To understand why these groups --IRA, ETA and the Maquis-- were successful, we have to look not only at their formal and informal policies regarding snitches, but at the movements as a whole. There is precious little written in English about ETA, but from the few sources available, *Clean Hands*, *Dirty Wars*, it seems that ETA has been able to avoid widespread Snitch Culture by the very nature of its resistance. It is heavily family- and community-based; nearly everyone knows everyone else and every Basque community has been affected by the draconian repression of the Madrid-State. Since most Basque are deeply attached to their homeland, even the non-nationalists, the idea of snitching on neighbors and comrades is wrought with practical difficulties. Raising the stakes for squealing, neighbors, co-workers and friends would react negatively to the appearance of a snitch, and so anyone caught snitching would not only have to create a new social circle, but relocate.



The IRA put a tremendous amount of energy into prisoner support. In fact it was estimated by Gerald O'Mann that nearly a 1/3 of all money raised by the IRA was spent directly on prisoner support. The Irish nationalist concept of prison support is more extensive than ours and includes family support, the glorification of prisoners, treating ex-prisoners like returning veterans, as well as in-jail support. An IRA prisoner was even elected to parliament while still in jail! This support seriously diluted the benefits of snitching and the consequences (often violent reprisals) greatly outweighed the benefits. The IRA, more than any other group, was successful in reducing the punitive nature of incarceration.

The Maquis used a combination of violent attacks on snitches as well as "reframing" propaganda. There is much written about the beatings and shootings carried out by Maquis, but the historic record actually shows that the Maquis ability to carry out such attacks was extremely limited. They made use of very public reprisals, in no doubt due to the monopoly on news by the occupiers, which, in turn, increased their effectiveness. However, the use of violence can only be seen as a partial explanation for the success of the Maquis in resisting Snitch Culture. The Maquis used an effective propaganda that was based on the idea that they soon would be victorious, which made less attractive the cooperation with illegitimate authorities that would soon be removed. What is surprising when one reads the memoirs of resistance fighters and the historical accounts of everyday French living under occupation is their firm and unshakeable belief that they would be liberated. In fact, most French not only believed they would be liberated, but liberated by the combined French Resistance forces. This belief gave legitimacy to the Maquis and made crossing them a more consequential prospect, since they believed they would come to power-- which in fact many did.

In our own present Communities of Resistance there seems to be no clear theory or discipline regarding the issue of snitches, however, as Anarchists, our inherent critique of authority and power, knowledge of security culture, and decentralized style of organizing are certainly beneficial in fighting Snitch Culture. That said, the few approaches we have used in dealing directly with snitches have not been very successful. We seem to mainly operate under some loose code somewhat akin to the "Revolutionary Discipline" of the RAF. The idea that 'Snitches get Stitches' is prevalent and agreeable to our politics, however it is impractical in that we lack the sheer numbers -- both inside and outside of the jails-- to make this a reality. 'Snitches get Stitches' functions more like the WU idea of terror and with the exact same results in preventing Snitch Culture: absolutely none. Knowing this, communities have also tried the BPP model of shame, but with the recent evidence of government infiltration of radical groups and organizations, former comrades turning into collaborators with wiretaps, and friends arrested or under Grand Jury subpoenas naming names and cooperating with authorities, there is ample evidence that this too is ineffective and unlikely to stem the continuing tide of snitches.

It is easy to look at all of this and grow desperate. Snitch Culture is not a problem that can be easily solved and the very issues at the core of it run right through the heart of everything we are attempting. And perhaps that is the question and answer to this issue: what are we

attempting? Why are some groups, like ETA, the IRA, or The Maquis able to successfully deny attempts by those in power to fracture and break their cultures of resistance? Why do Anarchists, with the goals of destroying power and creating a new world of freedom and mutual aid, turn into 'cooperating witnesses' and sacrifice not just their own dreams but those of the communities they belong to?

These are the questions we must ask ourselves if we want to build Communities of Resistance that will hopefully, one day, win. We must think of ways to strengthen our communities of autonomous individuals and build a resistance that is effective and sustainable in the long-term, instead of the current haphazard and reactive scrambling to each and every blow of government repression.

What we can learn from the Communities of Resistance that were successful in defeating Snitch Culture is that they believed wholeheartedly in their struggle. Those that were actively fighting, as well as those who supported them, did not see any choice but to liberate themselves from illegitimate authority and therefore saw themselves individually as part of something larger. This should not be read as a call for individuals to sacrifice themselves on the altar of the collective, but to illustrate that people who believe in what they are fighting for, and identify themselves personally with the success or failure of that fight, are less likely to betray that struggle because that struggle IS them.

However, it must be said that it is probably easier for people to identify intimately with national liberation struggles that have --in a sense-- simpler goals, than with something as complex and far-reaching as Anarchy. The Maquis wanted to overthrow the Nazi-collaborator Vichy government and to oust the German occupiers from France. The IRA wants to kick the English out of Ulster. ETA wants autonomy from Spain and France and to preserve the Basque language and culture. These groups are fighting against one particular source of power, whereas Anarchists are struggling to destroy all power.

Considering the fact that Anarchy is more than just the liberation from one particular illegitimate authority and there are as many battlefields as there are stars in the sky, it can become easy to feel disillusioned or ineffective. After all, authority and capitalism still exist and we are drowned in the propaganda that we have reached the End of History; that the Way Things Are will continue unabated, forever. Snitches in Communities of Resistance are often people whose identity with the struggle for total liberation has become fractured, or those who, in the face of the repressive power of the state, betray their communities because they feel there is little chance those communities can win.

If we are to defeat Snitch Culture in our Communities of Resistance, we must refute the propaganda of those in power. It means tearing up the history books because the end is not predetermined by anyone but us. The ways and means of building a resistance

that can refute their history and can engage in a sustainable and long-term struggle for freedom, are the same ones needed to give Snitch Culture the final blow. Clearly, the solution is not as simple as the suggestion 'Snitches get Stitches,' but is complex and takes us in many directions.

As detailed earlier, there have been plenty of failed experiments in dealing with the issue of snitches and the current epidemic of snitching cannot be stopped through random beatings or through empty threats. While violence against snitches or collaborators may be necessary (for example, the very public targeting of snitches utilized by the Maquis could prove useful) it is often harmful or useless in ending Snitch Culture. Not only can the State outmatch us in terms of the violence it can expend, rendering moot a wholesale campaign of violent reprisals --as in the case of the RAF-- it also seems counter to our politics of freedom to use the idea of terror to coerce people into line and could put off sympathetic or interested individuals --much like the WU did. This should not be read as a dismissal of the tactic of violence in our resistance, but as strong critique of violence as a useful tool in combating Snitch Culture.

What has the greatest possibility of working --although it is currently not practiced to the extent that it needs to be-- is community shame coupled with prisoner support. Community shame has the benefit of not being irrevocable --how can you make amends for shooting or beating someone terribly if it turns out they were wrongly accused?-- as well as providing a powerful disincentive for snitches by denying them friendship and support. Prisoner support is obviously positive in that it helps remove the power of violence that the State holds over people. Prisoners who feel supported and know they will be cared for have less reason to abandon their principles and betray their friends. Coupled together, a strategy of strong communities of autonomous individuals that will not allow collaborators back in, along with a prisoner support in which the benefits of not snitching far outweigh any measure put forth by the State, seems to be the best course of action. Presently, however, these tactics have proved ineffective in the prevention of Snitch Culture. Snitches know that they will be reviled by some, but they can remain in our communities by moving to where they may be anonymous or because there are people who will not ostracize them and allow them to return. And even though our prisoner support is one of our strongest attributes, it fails to be the linchpin that prevents Snitch Culture, mainly because it is limited in scope.

What this leads us back to is the idea of building stronger communities capable of long-term resistance to the powers of the State. Community shame and prisoner support lack their necessary bite precisely because our Communities of Resistance are fractured, with no real communication or trust amongst groups. In tightly-knit societies like the Basque, snitches have nowhere to go because word will travel and they would face social isolation wherever they go.

Shame only works when communities can communicate in a way that is informative and trustworthy. Without information about snitches, communities cannot take steps to isolate or shame that person; and without trust, communities have no idea if the information is reliable or that others will also take steps to ostracize a snitch.

IN THE STREETS
AT SCHOOL
ON THE JOB

EVERYONE
HATES A SNITCH.

In terms of prisoner support, our current Communities of Resistance offer a heartfelt support; however, due to our lack of infrastructure and support outside of traditional Anarchist circles, we cannot provide the all encompassing prisoner support of the IRA. For instance, in most cases, we cannot offer jobs, money to families, or pay for legal representation. Most prisoners are shunted from public view and only a few are known on a national or international basis. On the contrary, IRA prisoners were glorified and at the height of the Troubles, the majority of the murals in IRA neighborhoods were dedicated to celebrating prisoners and their deeds. The culture of prisoner support in the IRA fostered an environment that made it desirable to not snitch, a desire based on a total community support for the prisoner and family. With some exceptions, this is something that we cannot currently provide.

Where this leaves us is on the brink of a solution. While we do seem to utilize the effective tactics in combating Snitch Culture --prisoner support and community shame-- they are not actually effective in stopping it. Snitch Culture is not an isolated problem, as mentioned earlier, but an interrelated issue with other problems facing our Communities of Resistance. It comes as no shock to hear that our communities are fragmented and that there is little communication or mutual aid between them. The same also goes for the lack of infrastructure or support of people not traditionally identified with Anarchists or other radical groups. We must seriously and critically examine our communities and search for ways that we can do things better, not just to defeat Snitch Culture, but to win!

"We must create strategies that look beyond today and will allow us to proactively deal with State repression, not only to defeat Snitch Culture, but to create a world made of our desires."



The way to strengthen our communities and increase our resistance to Snitch Culture would begin by practicing real mutual aid. Very few groups actually work together in a way that is interrelated and that would actually help build our counter-infrastructure. For instance, people in cities who want to grow their own food and those who already live on farms could participate in projects like the Victory Gardens in Athens, Maine, which helps disenfranchised people in both urban and rural communities develop their own sources of organic food; groups in different cities could pool money and have benefits to pay for the legal costs of prisoners in other places; and those choosing not to work could help provide daycare for working people who have to. The ways in which we can work together and support each other are limitless, and working together on projects and actions is a simple but unrivaled way to build trustworthy lines of communication based on experience-- as well as creating networks of autonomous communities that support each other and would not tolerate a snitch among them.

Infrastructure is important if we are to provide support for people in prison that would actually function as a deterrent to snitching. For instance, we cannot always give people jobs --if they want them-- when they are out, or provide for people's families if they are put away. The counter-infrastructure we do have is largely based on entertainment, and while this is a positive thing in our communities, we must move beyond this into other territory. For many obvious reasons, creating an infrastructure that does not rely on capitalism, but is our very own, is absolutely vital to our ability to wage effective resistance.

We must also address the lack of support for our resistance in communities outside of Anarchist circles. One way other Communities of Resistance have been effective is that they had a large network of support in larger society. Besides the obvious, this larger support functioned as a way to propel resistance and created a climate of hope --a climate that Snitch Culture does not function very well in. This lack of support may be due to the fact that our definition of Anarchist culture is rather narrow. Although not true in the least, the image of Anarchists as young black-clad punks certainly does persist and is to an extent perpetuated by Anarchist culture. Anarchists should proudly proclaim themselves, but should also move beyond the stereotype and show our many faces: young and old, queer and straight, crusty and freshly-showered.

And obviously, our current prisoner support must continue --and increase-- while working on the long-term projects of building infrastructure and widening our circles of support. Prisoner support needs to become something that everyone in our community is working on. Comrades must have the full support of their communities when facing down the courts, the jails, and the prison terms of the State. We need to make prisoner support public and visible, and we need to show comrades on the other side of the wall that they are not forgotten. Murals, benefits, sending letters and birthday cards, attending court dates, and solidarity events are all easy ways to show that we celebrate and stand behind those from our communities who are behind bars. We need to make good on the saying: they are in there for us, so we are out here for them!

It should be clear that there is no simple solution to the persistence of Snitch Culture in our Communities of Resistance. This zine set out to begin a dialog on how we can destroy Snitch Culture once and for all. As we have seen, we may currently be unable to prevent snitches in our fight for liberation because we lack the community support and infrastructure we need. This does not mean that we should ever, ever condone snitching. Snitching represents the most vile betrayal of one's self and one's community and although we may not be able to prevent Snitch Culture now, this does not mean that we should not continue in the active removal of snitches from our communities at present and withdraw support from all collaborators immediately. But now we know that this is not enough. To eradicate Snitch Culture we must set ourselves upon the task of building a long-term resistance that can withstand the attacks of power, and that will take time and a lot of hard work. We must create strategies that look beyond today and will allow us to proactively deal with State repression, not only to defeat Snitch Culture, but to create a world made of our desires.

Public Eye

- 1- Describe the ways informants and the fear of informants distort social movements. Have you seen this in your political work?
- 2- Describe the process by which an informant becomes a saboteur or a provocateur. What problems does this pose for the government? What benefits does it receive? How can activist groups recognize this dynamic? How should they respond to it? Can it be prevented?
- 3- Describe the process by which the RNC protest organizations confronted and cleared an informant. What mistakes did they make? How could the situation have been handled better?
- 4-At the end of the article, Cincotta claims that, due to informants "Civic participation is cut back. Allies such as churches will abandon groups under surveillance. Perceiving an increase in government repression, some activists quit entirely." Do you agree? Does repression automatically passivity? What factors may influence the impact of repression on organizations? On movements? On a populace?

Michael William

- 1-The interview subject says: "They attended all the meetings. . . they took notes. That clearly was suspicious. Those who do the most work are the most suspect."
Do you agree or disagree?
What about the other actions and characteristics of the informers -- claiming a history of direct action, wearing an anti-summit shirt, winning paintball tickets, being zealous and enthusiastic, buying supplies, providing funds, "mak[ing] violent statements toward the cops," bringing wine to a meeting, encouraging continuation of the group -- which of these was or should have seemed suspicious? Why?
- 2- Why did members of Germinal ignore the warning that they had been infiltrated? How could they have handled the situation better?
- 3-Members of Germinal offer several pieces of advice, explicitly or implicitly. List them. Is their advice good? What are its strengths, weaknesses, and trade-offs? How could the state circumvent their proposed security system? What organizational practices would you recommend to a group like Germinal?

Leader or Led? Anna and Eric McDavid

- 1- Describe Anna's role in the group.
- 2- What behaviors and traits did Anna exhibit that should have been worrying to her comrades? Were there other clues that they missed? How would you have responded to these clues?
- 3- How well was the group functioning aside from Anna's involvement? What were some of the problems? Were these people -- individually and collectively -- well suited to the type of activity they were considering? Why or why not?
- 4- How do you understand Zach and Lauren's decision to testify against Eric? How does this reflect the group's dynamics? Could their betrayal have been prevented?
- 5-What was this group's approach to security? Why did it fail? Did they suffer more from bad security or bad politics (or both)?

This American Life and Misogyny 1- What behaviors and traits did Darby exhibit that should have been worrying to his comrades? How would you respond to these behaviors?

2- How do you understand Darby's motives in becoming an informant? How did they differ from his motives in becoming an activist? How did they resemble them?

3- Why do misogynists make good informants? What does this suggest about the relationships between a group's politics, its internal dynamics, and its vulnerability to repression?

4- What remedies does Morris suggest? Can you think of others? How is your organization employing these countermeasures? How can you improve?



David Paul Morris/Getty Images

From Movements to Mosques, Informants Endanger Democracy

By Thomas Cincotta
The Public Eye, Summer 2009

[ShareThis](#) | [Printer Friendly](#)

Thomas Cincotta is civil liberties program director of Political Research Associates and a member of the Public Eye editorial board. His blog, Liberty Beat, tracking repression can be read at www.publiceye.org.

In February, 2009, members of the Islamic Center of Irvine learned that the Federal Bureau of Investigation (FBI) had hired Craig Monteilh, a 46-year-old fitness instructor and convicted con man, to infiltrate their mosque and keep it under surveillance. Members had wondered about Monteilh for a while. Back in 2007, the local chapter of the Council on American-Islamic Relations (CAIR), alarmed by his talk of *jihad* and plans for a terrorist attack, reported him to Irvine police and secured a three-year restraining order against him.

The news that Monteilh not only infiltrated the Irvine mosque but mosques across Orange, Riverside and Los Angeles counties came out during a bail hearing for Ahmadullah Niazi. [1] Niazi, an Afghan native and U.S. citizen, was up on charges that he had lied about ties to terrorist groups on immigration applications, because he did not disclose that his brother-in-law was Osama bin Laden's bodyguard, and that he traveled to Pakistan in 2005 where he allegedly met with a terrorist.

RELATED AUDIO

[Listen to Public Eye editor Abby Scher's interview with Thom Cincotta. \(MP3\)](#)

The Public Eye MAGAZINE

Summer 2009
Vol. 24, No. 2 :

- [Front Page](#)
- [From Movements to Mosques, Informants Endanger Democracy](#)
By Thomas Cincotta
- [Remembering the New Right](#)
By Richard J. Meagher
- [Battle over Labor Law Reform Shows True Power of the Right](#)
By Abby Scher
- [Letter to the Editor](#)
- [Book Reviews](#)
- [Reports in Review](#)
- [Eyes Right](#)

[The Public Eye](#)
[Subscribe Online](#)

End Notes

1. Salvador Hernandez, "Tustin Man Suspected of Terrorist Ties Pleads Not Guilty," *Orange County Register*, March 2, 2009.
2. Gillian Flaccus, "*Calif. case highlights use of mosque informants*," *Associated Press*, March 1, 2009; Matt Coker, "A look at Craig Monteilh," *OC Weekly*, March 4, 2009; Teresa Watanabe and Paloma Esquivel, "L.A. area Muslims say FBI Surveillance has a chilling effect," *Los Angeles Times*, March 1, 2009.
3. Gary T. Marx, "Thoughts on a Neglected Category of Social Movement Participant: the Agent Provocateur and the Informant," *American Journal of Sociology* 80 (Sept. 1974) pp. 415-421, p. 434.
4. Gregory F. Treverton, *Reorganizing U.S. Domestic Intelligence: Assessing the Options*, (New York: RAND Corporation, 2008), p. 7.
5. This year's National Fusion Center Conference featured a closed session on the radicalization phenomenon and "understanding the process that leads a person to support and/or pursue violence." U.S. Dept. of Homeland Security, 2009 National Fusion Center Conference, March 10-12, 2009.
6. Randy Furst, "Terrorism charges against RNC 8 are dropped," *Minneapolis Star Tribune*, April 10, 2009.

Posing as a new convert, Monteilh arrived at the Irvine Islamic Center in 2006 wearing robes and a long beard, using the name Farouk Aziz. Monteilh had a long rap sheet and had served 16 months in state prison on two grand-theft charges. But he found new friends in government in his new role. FBI Special Agent Thomas J. Ropel III testified that Monteilh recorded Niazi on multiple occasions, talking about blowing up buildings, sending money to the mujahedeen, and acquiring weapons, although the government has not charged Niazi with terrorism. Niazi is said to have refused to become an FBI informant after he complained to the agency about Monteilh. [2]

We don't yet know if Monteilh's talk of *jihad* egged Niazi on. Was he an *agent provocateur*, like the two well-paid FBI informants in the 2006 Sears Tower terror plot, supposedly concocted by men from Miami's deeply impoverished and predominantly black Liberty City neighborhood? After two hung juries, in May a third jury finally convicted five out of the six defendants for planning to blow up the Chicago landmark. The New York Times quoted a law professor as saying, "It goes to show that if you try it enough times, you'll eventually find a jury that will convict on very little evidence." Previous juries viewed the FBI informant posing as a member of al Qaeda as the driving force behind the plot. Despite paying informants over \$130,000, the FBI produced no evidence of explosives, weapons or blueprints, only a videotape of defendants pledging an "oath" to al Qaeda, recorded in a warehouse wired by the FBI. The defendants are petitioning for a new trial.

Since the government's use of secret informants is increasingly visible, in mosques and in an array of activist networks, so too are questions about whether the spies instigated events and infringed on people's constitutionally protected rights to free speech, association, and privacy.

In a dozen or so cases exposed within the last few years, informants facilitated bomb-making, provided logistical support, cajoled others with provocative language, and goaded people to break the law. Not every informant can be blamed for provoking illegal activity, and entrapment is a difficult thing to prove. Targets of surveillance do often plan or commit crimes: witness the five men sentenced to life terms in April 2009 for their role in plotting an armed assault on Fort Dix in New Jersey. Yet, even in that case, informants played key roles in planning those crimes.

By and large, evidence shows informants do not merely observe and collect data. They make things happen. Their mere presence creates distrust and conflict, making them an efficient tool of repression that in recent years has affected broad, predominantly Muslim communities in the United States, as well as left-wing activists. Informants can cause confusion and dissatisfaction among members of groups and communities they infiltrate, discrediting leaders, and fostering factionalism as people wonder if any of their colleagues are spies. Their handlers' structure of incentives – raises, promotions, transfers, financial rewards, waived jail time – creates a system where informants consciously or subconsciously create and then destroy terrorist threats that would not otherwise exist. These pressures can push them from passive observer to aggressive actor, with serious consequences for constitutionally protected free speech. Another unplanned result: government loses legitimacy and support in the eyes of targeted communities, if they feel they have been manipulated.

Today's informants carry the same disruptive potential as their counterparts in the FBI's 1960s-era counterintelligence program (COINTELPRO), which aimed "to expose, disrupt, and otherwise neutralize the New Left organizations, their leadership and adherents." [3] Today's agents are shrugging off constraints placed on them in 1976, after the program's illegal break-ins, assassinations, and dirty tricks against civil rights, antiwar and other activists were exposed. Following high-profile investigations, Congress limited the Bureau to investigating activists they believed were about to be, or were actually engaged in, criminal activity. [4]

But in the post-9/11 environment, intelligence gathering is driven by a theory of preventive policing: in order to anticipate the next terror attack, authorities need to track legal activities – much like the "pre-crime" units depicted in the film *Minority Report*. Pre-emptive policing dovetails with a police-promoted belief that "radicalization" is a key cause of violent extremism. [5]

This emphasis on prevention and radicalization blurs the distinction between thought and action by specifying ideological orientation as grounds for suspicion. It justifies investigating anyone or any group identified as fostering "subversive" ideas. It focuses not on crime, but on the possibility that a crime might be committed at some future date. This entire approach conflicts with the democratic notion – enshrined in the Constitution and numerous Supreme Court decisions – that government may not inquire into or restrict thought and speech.

Attorney General Eric Holder has not stated whether he will revisit lax Bush-era guidelines (see box). Despite the availability of alternative, less constitutionally "iffy" investigative techniques, the use of informants appears to remain a favorite tactic – not only of the FBI, but, as we know from 2008's political conventions, local police as well.

AGENTS PROVOCATEURS AT THE RNC

Few civil liberties advocates were surprised when they learned police had deployed informants before and during the 2008 Republican National Convention in St. Paul, Minnesota. Both the FBI and the Ramsey County Sheriff's Department dispatched informants to spy on protest organizations. Their efforts eventually led to the arrest of eight activists prior to the convention on charges of conspiring to commit illegal acts. While the county prosecutor dropped terrorism charges against them in early April, the RNC 8 still face felony conspiracy charges that they promoted riot and property destruction in an effort to "shut the city

COMMON SENSE SECURITY

Political dissidents and groups seen as "internal enemies" have always faced government repression. It is important to take these attacks seriously and object to them. At the same time it is important not to allow fearmongers to scare you away from civic and religious life. [Click here](#) for useful tip sheets created over the years.

In February, California mosques discovered the FBI had hired a con man to infiltrate their communities.

7. According to the *Minneapolis Star Tribune*, the reports documented internal strains, gripes and names of activists, but no talk of property damage.

8. Randy Furst, "Anarchist looked like someone's mom," *Minneapolis Star Tribune*, December 1, 2008.

9. Marx, p. 403.

10. Marx, p. 428. "Specious activists may help perpetuate a protest group by offering the kinds of resources and moral support that are often in short supply among those who take highly unpopular positions and engage in illegal actions. Because of their need to be accepted, agents often work very hard, are often very successfully at gaining new recruits for the movement, and even at starting new branches of a movement."

11. Revolution, "Political Persecution of the RNC 8: Part 2 Informants and Undercover Agents," March 11, 2009; Randy Furst, "RNC Informant Found Guilty in Minneaprista Assault," *Minneapolis Star Tribune*, March 23, 2009.

12. FBI Confidential Informant Guidelines, § II.A.1. A September 2005 Special Report of the Office of the Inspector General (OIG) found one or more Guidelines deficiencies in 87 percent of the confidential informant files it examined. OIG also noted failure by executive managers to hold first-line supervisors accountable for compliance deficiencies and exercise effective oversight of agents operating informants. See also Dan Eggen, "FBI agents often break informant rules," *Washington Post*, September 15, 2005, p. A15.

13. Diana Welch, "The Informant: Revolutionary to Rat," *Austin Chronicle*, January 23, 2009, p. 7.

14. Colin Moynihan, "Activist unmasks himself as federal informant in G.O.P. Convention Case," *New York Times*, January 5, 2009.

15. Austin Informant Working Group, "Austin RNC Informant Brandon Darby is Provocateur Not Hero."

16. Marx, p. 421.

17. M. McMann, "The Police and the Confidential Informant," M.A. thesis, University of Indiana (1954) in Marx, *supra*, p. 416, n.17.

18. Marx, p. 420.

19. Austin Informant Working Group, "Austin RNC Informant Brandon Darby is Provocateur Not Hero," "Prominent Austin activist admits he infiltrated," radio interview.

20. Austin People's Legal Collective unofficial verbatim notes of McKay's trial.

21. Frank Donner, *The Age of Surveillance* (1971) as quoted in Marx, p. 434.

22. The jury acquitted them of attempted murder.

23. Amanda Ripley, "The Fort Dix Conspiracy," *Time*, December 6, 2007.

24. Geoff Mulvihill, "Informants' action key in Fort Dix terror case," *Newsday.com*, May 10, 2007.

25. Stephen Lendman, "The Troubling Case of the Fort Dix Five," *Counterpunch*, December 31, 2008.

down." The trial is expected to begin in September 2009. [6] But activists and civil libertarians have already learned about tactics that cause grave concern about the protection of free speech rights.

The spies filed about a thousand pages of reports for an investigation that cost \$300,000 to the county alone. [7] The sheriff's three undercover operatives are notable for their diversity: a female narcotics officer in her 50s, a 20-something female jail guard, and a headstrong muscular guy looking to be pushing 30.

Marilyn Hedstrom, the narcotics officer, introduced herself to anarchists as "Norma Jean Johnson" in August, 2007, telling activists she had issues with Bush and the Iraq war. [8] She cooked meals, ran errands, worked the security detail, and represented the organization at gatherings. Her reports show no talk of property damage or even protests at meetings she attended, but much discussion of internal strains, gripes, and names of activists.

CHANGES IN JUSTICE DEPARTMENT GUIDELINES NEEDED

Today many of the abuses of COINTELPRO are no longer illegal. Break-ins, wiretaps, and mail covers have been supplanted by national security letters and "sneak and peak" searches, authorized under the USA Patriot Act enacted after 9/11. The danger of these intrusions to privacy and free speech is magnified by the expansion of the domestic security apparatus. The fruits of surveillance can flow rapidly through 70 state intelligence fusion centers, channeling information across jurisdictions from local police to national security agencies.

The election of Barack Obama does not portend a sea change in domestic intelligence policy. There are no signs that his administration is rolling back definitions of terrorism stretched to encompass acts of nonviolent civil disobedience. [39] FBI Director Mueller, who serves a ten-year term, worked with former Attorney General Mukasey to issue new Guidelines for Domestic Operations in 2008 that:

- Authorize agents to attend meetings of a religious or political nature without any suspicion of criminal or terrorist activity;
- Decrease internal supervision and coordination at various stages of investigation;
- Expand the scope and duration of preliminary inquiries that turn up nothing;
- Permit agents to misrepresent themselves and conduct "pretext interviews" to elicit information; and
- Encourage the use of more intrusive techniques with no sense of prioritization. [40]

Informant Rachel Nieting, a guard in the county jail, accompanied Hedstrom posing as her niece, but did not fit in. Complete with a fake Facebook page under the alias "Amanda," Nieting did not gain the same level of acceptance from the anarchists as Hedstrom had, and dropped out. Hedstrom covered for "Amanda," explaining that she found a new boyfriend.

In their various roles, undercover agents can seriously distort the life of a social movement, as sociologist Gary Marx has argued. [9] Hedstrom and Nieting's participation made the organization seem larger and more inclusive. Nieting wrote that she and Hedstrom were the only two women to join Karen Redleaf at a women's caucus. Redleaf, a committee member, talked about how disconnected she felt and said was only coming to Sunday meetings because "Norma Jean" was there. [10]

The third informant, Chris Dugger, had tattoos and resembled a biker. He portrayed himself as participating in a radical movement for the first time. Still, he was accused by another member of being a cop. Denying the charge that he was an informer, Dugger became visibly emotional, wiping his eyes, blowing his nose, and telling the group how bad he felt. He must have been convincing, since two of the anarchists later told him "a cop would have just walked away and never returned and wouldn't cry."

By August, 2008, Dugger reportedly urged one anarchist to suspect another of being an informer. This highly disruptive practice, known as "snitch-jacketing," was a common tactic of COINTELPRO operatives. Snitch-jacketing not only stirs distrust, but can also provoke violence. For his efforts, Dugger's handlers won him a job in the county jail.

The FBI's informant, Andrew Darst, infiltrated the "action faction" having been first seen in anarchist circles three years before. He became active in committee meetings of the RNC Welcoming Committee and reported on events held by other, nonanarchist organizations. Not only did he record meetings, his apartment in Minneapolis was wired for audio and video recording. [11] In March, 2009, Darst pled guilty to two counts of misdemeanor assault and one count of property damage after breaking into a house by ripping the door off its hinges, confronting his wife, and striking two men present.

But this Minnesota-based spy was not the only person the FBI deployed to track people planning to protest the RNC. The example of Brandon Darby, a magnetic, discontented Texas activist, reveals how easily the fuzzy line between informer and instigator can be crossed.

THE DARBY CASE

For eighteen months before the 2008 RNC, the FBI paid more than \$11,000 to Darby, a gun-toting, outspoken Texas radical, to spy on fellow activists in Austin and then St. Paul. Darby was a charismatic leader with a reputation for defying authority who infiltrated the Austin Affinity Group for the FBI after becoming disgruntled with anarchist tactics. Government infiltration by a respected leader, handled by an FBI agent untrained in handling informants, presented the perfect setting for an agent provocateur to thrive.

Darby's deep involvement illustrates the pressures inherent in the informant's role. Informants must choose between being passive observers who yield sparse information and wield little influence, or more active participants who produce better information, but also affect what happens more directly – raising the risk of possible complicity and entrapment.

26. Nick Juliano, "Entrapment? Five convicted in Ft. Dix plot," *Raw Story*, December 22, 2008

27. Dr. Ian Lustick, Statement on the Fort Dix Terror Plot case, December 22, 2008.

28. Frank Donner, *The Age of Surveillance: The aims and methods of America's political intelligence system* (New York: Vintage, 1981) p. 7.

29. Amory Starr, Luis Fernandez, Randall Amster, "The impact of surveillance on the exercise of political rights: an interdisciplinary analysis 1998-2006," *Qualitative Sociology* 31, (July 2008), pp. 251-270

30. Starr, *et.al.*

31. Donner, p. 6.

32. Starr and Fernandez, p. 15.

33. Teresa Watanabe and Paloma Esquivel, "L.A. area Muslims say FBI surveillance has a chilling effect," *Los Angeles Times*, March 1, 2009.

34. Samantha Henry, "Some Muslims Rethink Close Ties with Law Enforcement," *Associated Press*, May 4, 2009.

35. David Cole, *Enemy Aliens* (New York: New Press: 2003), p. 183.

36. Donner, p. xv.

37. Lisa Rein and Josh White, "More Groups Than Thought Monitored in Police Spying: New Documents Reveal Maryland Program's Reach," *Washington Post*, January 4, 2009, p. A01.

38. Barack Obama, victory speech after primary, South Carolina, January 26, 2008.

39. Nancy Chang, *Silencing Political Dissent*, Seven Stories Press, 2002, pp. 112-113. See e.g., Dane E. Johnson, "Cages, Clinics, and Consequences: The Chilling Problems of Controlling Special-Interest Extremism," *Oregon Law Review* 86 (2007), pp. 249-294.

40. James X. Dempsey, "Anti-Terrorism Investigations and the Fourth Amendment After September 11: Where and When Can the Government Go to Prevent Terrorist Attacks?" Statement before the House Committee on the Judiciary, May 20, 2003.

41. Jennifer Van Bergen, "FBI confidential informant also said to be provocateur," *The Raw Story*, June 8, 2006. Anna was also the subject of an *Elle* magazine investigation in its "Green Issue." Andrea Todd, "The Believers," *Elle*, May 2008, pp. 266-325.

42. Dennis Walsh, "Student's path to FBI informant," *Sacramento Bee*, September 13, 2007, B5.

Spotlight On

Civil Liberties & Repression
Economic Justice
LGBTQ Equity
Racial Justice
Reproductive Justice
Christian Right & Theocracy
Understanding the Right

On the eve of the convention, two activists under Darby's surveillance, 22-year old David McKay and 23-year-old Bradley Crowder, concocted eight Molotov cocktails and stored them in a basement. Crowder pled guilty in the fall of 2008, but McKay's case went to trial. The jury split evenly on the issue of whether Darby, the elder turncoat, had entrapped him. McKay eventually pled guilty before his second trial began, saying he would have made the Molotov cocktails even without Darby's encouragement. But the question remains: Were the two men egged on by the charismatic Darby?

Darby was a self-identified revolutionary who slept with a gun under his pillow, according to friends. In the aftermath of Hurricane Katrina, he took an AK-47 and a handgun to New Orleans to help rescue an old friend in a neighborhood inundated by muddy water and White militias. He was a leader of the Common Ground relief effort in New Orleans and a member of the Austin activist community for more than ten years. Friends in New Orleans say he openly supported the use of firebombing as a tactic.

Given the need for informants to observe rather than lead, it is curious that the FBI found someone like Darby suitable for the task. Guidelines require the Bureau to evaluate the potential informer's motivation, dangerousness, and the extent to which the FBI can ensure that the information gathered is related to criminal matters. The guidelines do not address the potential for provocation *per se*, but FBI Agent Timothy Sellers said he cautioned Darby not to take a leading role. [12]

Sellers charged Darby with spying on a range of Austin-area activists, particularly the Austin Affinity Group. [13] Darby gathered information on a number of people engaged in lawful activism, including some who had no plans to attend the Republican Convention. He described meetings with his affinity group and people in Austin, Minneapolis, and St. Paul for the FBI. At times he wore recording devices, including a transmitter embedded in his belt. Four months before the RNC, he went to Minnesota and provided detailed narratives to authorities on meetings with activists from New York, San Francisco, Montana, and elsewhere. [14]

"The wider net cast by Darby in his information gathering shows that he was part of an FBI campaign to suppress political dissent and activism," said Will Potter, a journalist with the alternative press. "By gathering information on law-abiding activists and then defending his actions as stopping violence, Darby contributes to the public perception that political dissent is criminal, which has a chilling effect on free speech." [15]

Sociologist Gary T. Marx's study of *agents provocateurs* and informants suggests that the nature of informing may lead the informer beyond his or her assigned task, particularly when the motivation is personal or ideological. In his study, Marx identifies the potential motives of informants, including patriotism, coercion, financial reward, disaffection with activists, double agents who want to assist the movement, converts who lose their zeal, and provocateurs who find success in the role by exceeding their mandate. [16]

After returning from a trip to Venezuela, Darby said, he began to see major problems with "violent elements" of the movement and actions being planned by the RNC Welcoming Committee. Explaining his motivation to work for the FBI, he said he merely wanted to protect the Republicans' right to participate in the political process.

Ideological motives may produce poor information, says Marx. Disgruntled informants tend to exaggerate or even lie: "There is no limit to which people will go to get even for a real or imagined wrong." [17] Darby shared his employers' assumptions that anarchists were determined to use violence. "Such agents may thus feel free to encourage activists to take violent action or to report false information. They may feel that the group poses such a severe threat that any means (even lying to superiors) are necessary to destroy it," warns Marx. [18]

The FBI did not require Darby to shed his revolutionary fervor. Militant language and a reckless temperament remained part of his public persona. According to Lisa Fithian, who worked with Darby for a number of years, "Brandon was always provoking discord and aggression, in the antiwar movement in Austin in 2003, in protests in Houston against Halliburton, and in disaster relief at Common Ground in New Orleans." [19] At his first meeting with McKay and Crowder, he said, "I'm going to shut this f..ker down" and "any group I go with will be successful." Darby lambasted the two for looking like a bunch of "tofu-eaters" who needed to "start eating meat and bulk up" so they could fight. [20] In fact, he trained them in martial arts.

There was no reason for Darby to tone down his rhetoric as an informant, although such language could inspire illegal action by younger colleagues. The informant's secret status frees him or her from the constraints with which more prudent activists contend. Just as Monteilh championed violent *jihad*, Darby could express militancy without fear of reprisal. As Frank Donner observed, "the infiltrator's secret knowledge that he alone in the group is immune from accountability for his acts dissolves all restraints on his zeal." [21]

One of Darby's big moments came after the FBI seized shields that the affinity group made to use in blocking streets during the Republican Convention. Darby told McKay, "We're not going to take this lying down. You've got to do something about it." The next night, McKay and Crowder bought materials for Molotov cocktails. Darby claims that he urged restraint. When McKay considered hurling the Molotov cocktails at police cars parked at a station, Darby texted him, "It's your call. I support you making whatever choice you are comfortable with. Be proud of yourself for your work and take a chill." When McKay suggested that there were too many police around, Darby texted, "it's all good, sometimes it's best to fight another day ... - it's ok, I'll support you."

The government loses support among targeted communities if they feel manipulated by the use of secret informants.

Disgruntled informants tend to exaggerate or even lie, producing poor information.

More Article Topics

Explore

Selected Topics

[Browse Topics](#) | [Site Guide](#) | [Multimedia Bookstore](#) | [Magazine](#) | [Publications](#) | [Activists Resources](#)

Political Research Associates

- [About Us](#)
- [PRA News](#)
- [Watch short videos about PRA](#)
- [Donate!](#)

PRA IS AN AFFILIATE OF:

- [Causes in Common](#)
- [Talk to Action](#)
- [Open The Government](#)
- [Building Human Rights](#)
- [Stop Spying](#)
- [Other Allies in Activism and Research](#)

COPYRIGHT INFORMATION, TERMS, AND CONDITIONS

Please read our [Terms and Conditions](#) for copyright information regarding downloading, copying, printing, and linking material on this site; our disclaimer about links present on this website; and our privacy policy.

Updates and Corrections

Although Darby wore a wire to transmit his conversation with McKay about the Molotov cocktails, FBI agents took notes but made no recording. This raised suspicion among jurors that Darby had crossed the line from surveillance to provocation.

INFORMERS AND MUSLIM AMERICANS

Informers generate suspicion deep into the communities under surveillance. “What these guys have done is create an environment where every person begins to suspect the other and with the infighting and inward suspicion, the community becomes its own victim,” said Shakeel Syed, executive director of the Islamic Shura Council in southern California.

Across the country in New Jersey, two FBI informers helped lead the five Duka brothers down a similar path, ending with their sentencing on April 28, 2009 for conspiracy to commit terrorism. [22] Authorities opened the Fort Dix file in 2006 after a Circuit City clerk showed police a video the brothers asked him to convert to DVD. On the video, camouflaged, bearded men shot semi-automatic weapons at a shooting range in the Poconos, where the defendants played paintball, skied, rode horses, and played videogames with their male buddies. On tape, the men shouted “Allahu Akbar,” meaning “God is Great.” Thinking the weapons were automatic, the clerk phoned police. In the eyes of the FBI, these were gun fanatics taping a training video or training for *jiḥād*. Had they not been Albanian Americans, the shooters’ bravado might not have raised suspicion. But in the post-9/11 world, the video offered cause for investigation. [23]

WHO IS ANNA?

“Anna” was an FBI informant for two years, who came to activists’ attention at a Fort Lauderdale protest of the Organization of American States (OAS) meeting in June, 2005. Ray Del Papa watched her, dressed as a medic with a red cross on her shirt and bag, directing young people to sit down in the street directly in front of a line of police in riot gear, using provocative language even though organizers had decided against sit-ins. [41] They had not counted on an informer in their midst. Anna went on to sleep with a young anarchist who was eventually given a prison sentence of 19 years and seven months for conspiring to sabotage a U.S. Forest Service genetics tree lab and nearby fish hatchery in Rancho Cordova, California. Juror statements that they felt unfairly hemmed in by the judge’s instructions on whether the anarchist, Eric McDavid, was “predisposed” to commit the crime before meeting the informant; that now forms some of the basis of his appeal. [42]

Rather than interview the brothers, or merely monitor them – investigative options that seem old hat in the informer age – the FBI dispatched two untrained civilians to ingratiate themselves with the men in the video. The first informer, Mahmoud Omar, was a convicted felon who entered the United States illegally in 1992 and faced fraud charges. The FBI told him they would clear his debts and help him obtain legal residence, and paid him \$238,000 for his undercover work. The second informant, Besnik Bakalli, received \$13,000 from the FBI, immigration assistance, and pardon for an old shooting charge from Albania.

Informant Omar was the apparent leader of any plot against Fort Dix. He organized “reconnaissance missions” in which he drove Mohamed Shnewer around potential targets while he railed against the United States. Omar stoked Shnewer’s fire, although he claimed during the trial that he was just trying to fit in. But Shnewer took the bait. On August 1, Shnewer told Omar, “If you want to do anything here, there is Fort Dix and I don’t want to exaggerate, and I assure you that you can hit an American base very easily...When you go to a military base, you need mortars and RPGs.” Omar offered to turn such fantasies to reality, promising to introduce his comrades to an arms dealer and giving them a list of weapons he could procure.

The recordings stretched out over a month, during which Omar badgered defendant Serdar Tatar to get him a map of Fort Dix. Tatar eventually did – but not before he called Philadelphia police to report being pressured for the map and voiced concern that it could be terror related. [24]

Without the FBI’s *agents provocateurs*, there might never have been a plot or weapons. Transcripts record some defendants explicitly rejecting violence. In a conversation recorded in April, 2007, Dritan Duka rebuffed Bakalli’s appeals for violent action. “We are good the way we are,” he tells him. “We are not going to kill anyone. Even if we kill anyone, you can’t run away. They will catch you right away.” But this did not deter the informers. At some points, the defendants seemed too scared to do anything. When they were supposedly shopping for weapons, one defendant worried that “as Muslims, if we get caught, we all get sent away to f...ing Guantanamo Bay for ten years with no court date.” [25] Nevertheless, several defendants were caught on tape talking callously about killing as many soldiers as they could in a fantastic assault on the Fort. FBI arrested the six after the Duka brothers bought seven high-powered rifles in a deal set up by Omar.

“Many in the Muslim community will see this as a case of entrapment,” said Jim Sues, executive director of the New Jersey chapter of the Council on American-Islamic Relations (CAIR), who attended the trial. “From what I saw, there was a significant role played by the government informant.” [26] Dr. Ian Lustick, political science professor at the University of Pennsylvania, notes that, Ever since 9/11, national, state and local authorities have tried with enormous resources to find, prosecute, and punish Muslim terrorists inside the United States. The result has been an increasingly embarrassing string of trumped-up charges that trigger much War on Terror warrior chest-pounding, and screaming, terrifying headlines for weeks following the arrests and indictments. Then, months or even years later, when evidence is put before juries and the public, we find that the real “perpetrators” were the paid government informants, seeking profit by inciting and enabling cheap talk and any acts they can produce by gullible, emotional and foolish suckers. [27]

Informants can promote militancy without fear of reprisal from the government.

THE IMPACT ON MOSQUES OR MOVEMENTS

Whether in a mosque or a movement organization, informants achieve the same results: demoralization, helplessness, cynicism, and immobilizing paranoia. After Brandon Darby admitted spying on his friends, Lisa Fithian told *Democracy Now*, “We feel traumatized. We feel as if somebody that we thought actually had good intentions and cared for this community has been a lie.” Conventional invasions of privacy are alienating and even dehumanizing. But government surveillance goes further, tampering with the very group dynamics through which political change is brought about. [28]

According to a recent study by sociologists Amory Starr and Luis Fernandez, government surveillance causes activists and citizens to fear participation in completely legal events and to be reluctant to donate to organizations, sign petitions, and receive newsletters. Civic participation is cut back. Allies such as churches will abandon groups under surveillance. Perceiving an increase in government repression, some activists quit entirely. Those who remain active find an organizing culture that was once open is replaced with a “security culture,” complete with reduced discussion, less note-taking (since it makes people look suspicious), and more secretive planning. A broad perception is created that activists’ political work is marginal, criminal, or suspicious. [29]

Inevitably, surveillance and even the fear of surveillance on the part of those not actually monitored produce a pervasive self-censorship. One activist described the effect: “I had to learn not to welcome people and not give out information . . . I’m interested in community building, and then you’re taught to be suspicious and not welcome people; it’s antithetical to your theory of change.” [30]

When a person’s politics come under hostile investigation by a secret police unit in a country like the United States that boasts of its freedom, it is traumatic, to say the least. The undercover character of the investigation, the assumed guilt of the person, the denial of an opportunity to answer any charges and confront the accuser, can all be shattering. People are made even more vulnerable by the secrecy of the probe and the knowledge that government may maintain a file on them for the rest of their lives. [31] The hallmarks of a security culture are exclusion, wariness, withholding information, and avoiding diversity. As Starr and Fernandez report: “It’s hard to build when you’re suspicious.” [32]

The same is true for Muslim communities – it is harder to organize if you are wary about others. Through the reckless use of informants, the government has actively cultivated distrust in both activist and targeted populations. “It gives you a little bit of apprehension about who you trust,” said Omar Turbi of the Islamic Center of Irvine. “Makes you think twice about what you say; what if people misunderstand you?” Hussam Ayloush, Executive Director of CAIR in Anaheim, added, “Some average Muslims interested only in praying are avoiding mosques for fear of somehow being monitored or profiled. Everybody is afraid, and it is leading to an infringement on the free practice of our religion.” [33]

Not only is freedom of religion being chilled, but the government’s use of informants is alienating Muslim Americans. As recently as this spring, allegations of widespread infiltration of mosques led several Muslim and Arab civil rights and community organizations to call for ending ties with law enforcement. [34] David Cole notes that “when law enforcement and intelligence officials treat a wide cross-section of the Arab and Muslim community as suspect largely by virtue of their ethnicity or religion, Arabs and Muslims will be less likely to cooperate with authorities and provided needed information.” [35] CAIR, the largest Muslim group in the country, had played an important role as liaison between the agency and Muslim communities.

Today many of the
abuses of
COINTELPRO are no
longer illegal.

DO INFORMANTS MAKE PEOPLE VIOLENT?

A team of behavioral scientists paid by the U.S. Department of Homeland Security is studying what turns radicals into violent extremists. But what about the influence of highly motivated informants? Paid informants are highly intrusive, aggressive, and potentially provocative. The ability of informants to neutralize democratic change and disrupt communities should raise concerns about whether pre-emptive policing is worth its social and political costs. As civil rights lawyer Frank Donner said, sizing up the surveillance through the 1970s, “under the warrant of protecting the democratic process from disruption and violence, the intelligence state is seriously jeopardizing it.” [36]

When Maryland activists learned that a state trooper infiltrated dozens of social justice groups over a fourteen-month period, they banded together with the ACLU and Defending Dissent Foundation to urge passage of a state oversight bill. [37] Social justice groups, including animal rights and environmental activists, must strengthen ties with Muslim, Arab, Middle Eastern, South Asian, and immigrant groups facing infiltration to demand constraints on how and when informants may be used to spy on Americans. Demands should include the use of less intrusive means of surveillance when a crime is suspected; independent oversight to ensure better supervision and training related to the use of informants for legitimate law enforcement purposes; and a ban on compiling dossiers on individuals and groups based solely upon their political, social or religious activities and beliefs. At a minimum, progressives must insist on re-establishing the protections instituted after the disastrous COINTELPRO programs, requiring suspicion of criminal activity as a threshold for government spying.

These are all in the best interests of the government, not just its citizens. In the long run, the government risks losing crucial support and legitimacy when its investigative tactics even *appear* to cross the line into provocation and unlawful investigation of protected First Amendment activities.

Candidate Obama explicitly invited Americans to mobilize as a counterweight to the “undue influence of the lobbyists” who “stand in our way.” [38] “I’m asking you to believe,” he said, “not just in my ability to bring about real change in Washington; I’m asking you to believe in yours.” For that energy and enthusiasm to coalesce into an organized political force, the Obama administration must rein in domestic intelligence practices that disrupt communities and discourage activism.

Portrait of a Police Infiltration

by Michael William

On April 18, 2001, two days before the start of the Quebec City Summit, two activists were arrested as they headed in a car toward Quebec City. Quickly, five more arrests took place of members of a group called Germinal.

I interviewed three members of Germinal in a Montreal café shortly before a demo in support of five members of the group who at that point (late May) were still in jail—they're now out on bail. The name of the fifteen-member group is taken from a novel by Émile Zola.

It had been the group's intention to use smoke bombs and "Thunderflashes" (military equipment that makes a grenade-like sound) to create a diversion which would have allowed a breach in the security fence to be made. Demonstrators would then have been in a position to enter into the off-limits area.

I began the interview by asking for a description of the group members' political outlook.

"The Germinal movement as such did not have a common ideology. Some were communists, or rather, Marxists; there were libertarians, anarchists, anarcho-communists. But there were also people you can't pin a political label on, who were simply citizens who were conscious of the anti-democratic nature of the FTAA and who were shocked by the police provocation: the wall, the six thousand cops present in Quebec City, and all the militarisation taking place there."

Because the group was clandestine and not openly recruiting, Germinal thought itself safe from police infiltration. Those involved, I was told, were "people we knew directly or through another person: so it was all people we knew. Usually in effect that's supposed to prevent infiltration of the kind we experienced. But they managed to infiltrate us anyway."

I asked the group to recount the infiltration.

"What is necessary to understand from the outset is that there is a traitor in the organisation. That is, someone who was not a cop but who went to the cops to let them know what we were planning. He did it to procure a personal profit. Without that we would never have been known."

A member explained the cops' modus operandi.

"They created a phony Montreal to Quebec City car-rental company. In the street where one of our members lives, flyers with job offers were distributed. I won't mention his name because he wasn't arrested. A very favourable moment was chosen to distribute the flyers: the person in question had just



Quebec cops defend themselves with shields at the anti-FTAA protests following the Germinal arrests.

lost his job, had left school, and was starting to be in dire financial straits. In addition the job offer was precisely in his field of interest: he's presently studying to become a truck driver. The offer paid well—seventy-five dollars per six-hour trip, which comes out to about \$15 per hour. So in December, 2000 he was hired. Afterwards, during a trip to Montreal, the person stayed at the apartment where I and Alex Boissoneault lived [Boissoneault was in prison at the time of the interview; he's presently out on bail]. The next day the cops, who were passing themselves off as company employees, showed up at our apartment. They said they needed another driver. So our friend Alex Boissoneault was hired. This was in the month of January."

"Next they began to hint that they were involved in ecological activism. The two cops were known to us as Nick and André. One of them, Nick, claimed to be a radical green. He said he had chained himself to a tree for 48 hours in British Columbia to keep it from being cut down. He wore a 'Fuck the Summit' t-shirt."

"So Alex took the bait and approached him. Nick became a member of the organisation like any other. Then Nick proposed that André be included. André was Nick's superior in the phony company. So in effect, André was included. But André's role

was more one of lending a helping hand with transport, money and material aspects, etc., etc."

"At this point they were just in contact with a few people. So they tried to widen the circle of people they knew in the movement. They said they had won tickets to play paintball and gave us twenty tickets to distribute to our friends. We were supposed to go out with them to have fun together. At that point they were able to meet other people in the group."

"Nick even took on certain responsibilities in the movement. He was very zealous and worked really hard for the project. He became the movement's

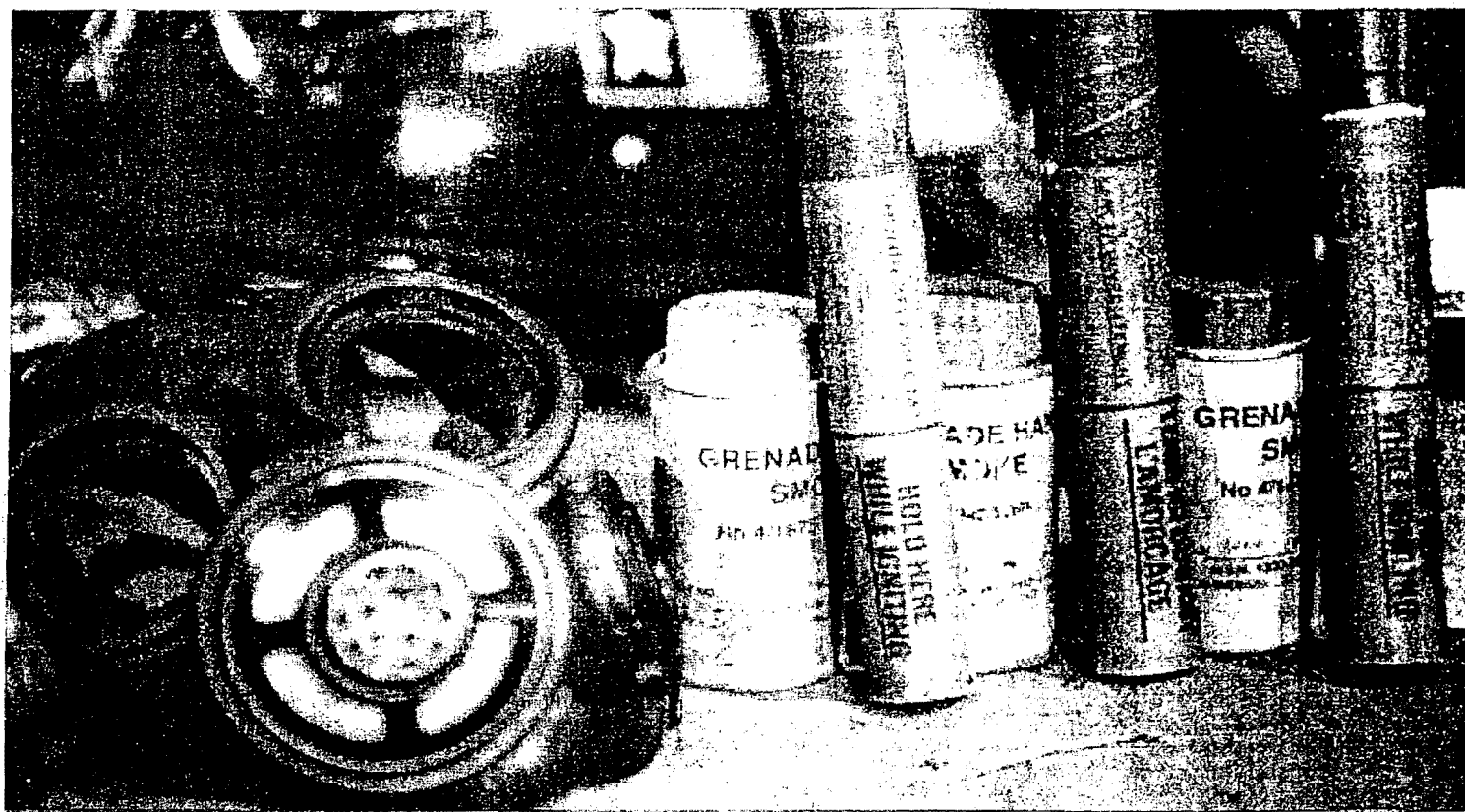
shopper when something needed to be bought. For example, we made some shields. Nick was the one who bought the styrofoam, tape and rope. He even loaned us his car. He furnished cell phones and helped financially."

"But he wasn't an agent provocateur. Let's say it was ambiguous: He was in between being a simple informer and a provocateur. He was an informer in the sense that he came to all the meetings. As a provocateur, at times he would make violent statements towards the cops. This made everyone uneasy because our goal was the wall and not the police; it was clear from the outset that we intended to hurt no one."

"The cops attempted to induce us to talk. At times even gross methods were used such as trying to get us drunk. Nick showed up at a meeting with two enormous jugs of wine. The scheme didn't work at all."

"He was very friendly. And we quickly became friends with him. He was a comrade like any other in the movement."

However, Germinal also had suspicions about the cops. "They attended all the meetings like any of us except that they took notes. That clearly was suspicious. Those who do the most work are the most suspect, we would say. But in the end we found it petty of us to suspect those who were doing the most to make the project work."



Material seized from Germinal is displayed at a police press conference. Photo: *Le Soleil*, Steve Deschênes

"At one point a friend of ours who has a relative who is a cop was at a family reunion. The relative told him: 'you know [Germinal member] Mario Bertoncini, we have people in his group.' We thought it was part of a campaign of intimidation. Also, we were afraid that if we told the others, dissention would make the group implode. We would start accusing each other of being cops. We would start attacking each other and being suspicious of each other."

Germinal's action at the summit was intended to be a one-off project following which the group would disband. Nick, however, argued that the organisation should become long-term: "He was always saying, 'it has to continue after, we can't stop there. We have to do other actions.'" When some members abandoned the group and those remaining wondered about the group's future and became depressed, Nick bolstered their spirits. "Nick was very, very enthusiastic. He would say, 'No, we're not giving up, we're going to continue on' and blah blah blah."

At the police press conference where material taken from Germinal was displayed, a number of items on the table were things that group had no intention of bringing such as steel balls accompanying slingshots. Whether to bring steel balls had in fact been debated at a meeting but it was ultimately

Because the group was clandestine and not openly recruiting, Germinal thought itself safe from police infiltration. Those involved, I was told, were "people we knew directly or through another person:...But they managed to infiltrate us anyway."

decided that paint balls would be used. "Except that the person who was supposed to buy the paintballs was Nick—one of the two double agents. He obviously was only too happy not to buy them. And the metal balls in question were furnished with the slingshot" (displayed in an unopened package at the police press conference).

One Germinal member had his own theory about why his group was popped as opposed to, say, one of the black bloc affinity groups. If one of the black bloc groups had been busted, he said, it would not have prevented the black bloc from acting which would have discredited the police, whereas,

"by arresting the people they arrested, they were sure of neutralizing the [Germinal] organisation."

"There was also the fact that there were people in the group who had a military background, former officers. That gave the impression that we were a paramilitary organisation which was not what we were at all."

A Germinal member also notes the convenient timing of the arrests. "We had been infiltrated since December and we were arrested two days before the summit." He said that the timing was media-motivated and to legitimise the vast police operation during the summit.

"Journalists later told us that the police press conference had been scheduled well beforehand. Several weeks previously the S.Q. (Quebec's provincial police force) approached certain journalists and told them, 'Soon, an event will happen that you absolutely have to cover.'"

"It's clear that we weren't prudent enough," a member said in retrospect. "We were naive. We were unaware of everything the cops and the state are ready to do to defend themselves, to defend their survival."

A member had the following parting advice for clandestine groups: "Always verify the people you're collaborating with."

- [Back To Results](#)
- [Previous](#)
- [Article 1 of 2](#)
- [Next](#)
- **Save this Article**

Leader or led by the FBI? - Attorneys paint contrasting pictures of defendant as the eco-terror plot case heads to the jury.

Sacramento Bee, The (CA) - Wednesday, September 26, 2007

Author: Denny Walsh ; Bee Staff Writer

A prosecutor told a Sacramento federal court jury Tuesday that Eric McDavid "was the driving force" behind an eco-terrorism conspiracy, and a defense lawyer countered that McDavid was entrapped by an undercover informant and the FBI agents working with her.

McDavid "never wavered from his belief" that violent action was required to get the attention of those who pollute and exploit the environment, Assistant U.S. Attorney Ellen Endrizzi told the jury in her closing argument.

She compared McDavid's alleged plan for a bombing campaign to the methods of the Earth Liberation Front and the Animal Liberation Front, radical environmental movements classified by the FBI as domestic terrorism.

But defense attorney Mark Reichel argued that McDavid did not come to the charged crime freely because he had fallen in love with "Anna," an FBI undercover operative posing as a member of the conspiracy.

"She was very good at deceiving people," he said. "She was on a mission to explore brave new areas of crime and report back to the FBI. Eric McDavid was not on a mission. He never had a chance.

"It was like a card shark and someone who didn't even know the rules of the game."

Two others charged in the conspiracy -- Lauren Weiner and Zachary Jenson -- did not have their hearts in a bombing campaign but were going along because they didn't want to let "Anna" down, Reichel told the jury in his closing argument.

Ticking off equipment, a log book in which the foursome recorded their activities, "the crisp \$100 bills" and a Dutch Flat cabin where the group lived in the days leading up to the trio's arrest -- all supplied by "Anna" thanks to her FBI sponsors -- Reichel said, "That's the creation of a case."

"Without 'Anna,' you have nothing," he declared. "That's entrapment."

But Endrizzi and Assistant U.S. Attorney R. Steven Lapham argued that "Anna" had little contact with McDavid before he told her of his planned campaign in the summer of 2005, while she was driving him to Chicago from an "anarchist" conference in Indiana. Thus, the prosecutors insisted, McDavid had a "predisposition" to violent action.

Lapham reminded the jury "Anna" testified that, on the same drive, McDavid told her, "If you're a cop, I'll kill you."

"Doesn't that comment tell you he was dead serious about the bombing campaign?" the prosecutor asked rhetorically.

Endrizzi argued that romantic feelings McDavid may have had for the informant are "a red herring." There was nothing physical between them, she said.

"The evidence is he was not reluctant" to proceed with the bombing campaign, she said.

Even if McDavid wanted to impress "Anna," that is "motive, not inducement," Lapham argued in his rebuttal of Reichel. The prosecutor said it makes no difference what McDavid's motives may have been, there was still a criminal conspiracy.

McDavid, 29, is charged with conspiring between June 2005 and Jan. 13, 2006 -- the day of the arrests -- to damage and destroy the U.S. Forest Service's Institute of Forest Genetics in Placerville, the Nimbus Dam and nearby fish hatchery in Rancho Cordova, and "cellular telephone towers and electric power stations" at unspecified locations.

The prosecutors on Tuesday pointed to the foursome's November 2005 meeting at the home of McDavid's parents in Foresthill as a pivotal event in the conspiracy.

It was then, they argued, that the agreement was struck to proceed with a bombing campaign

Weiner volunteered to buy "The Poor Man's James Bond," a book with instructions on how to build a bomb, the prosecutors reminded the jury.

Under the law, they said, a conspiracy is an agreement among two or more persons plus at least one overt act.

"The conspiracy was complete when Lauren Weiner bought that book," Lapham told the jury.

But Reichel argued that, without "Anna," there would have been no Foresthill meeting.

He reminded the jury that the FBI instructed "Anna" to get the threesome together and find out if they were serious about going ahead with the bombing campaign.

Trial evidence showed that Weiner did not have the money to travel from Philadelphia, where she was living, to the Sacramento area, and was afraid to fly. "Anna" paid for her round trip airfare and persuaded her to make the trip.

The evidence also showed that McDavid insisted family commitments prevented him from attending a meeting in the fall of 2005, but "Anna" insisted that he make time.

"She's there to focus them and get them to fix a target," Reichel said of "Anna." "The woman now has one single target, like a heat-seeking missile."

Further, Reichel argued, had it not been for "Anna's" urging and planning, the group would not have reconvened in Dutch Flat the following January.

"Take 'Anna' out of the equation, and they don't get back together," he told the jury. "The tumbleweeds" -- a reference to the vagabond lifestyles of McDavid and Jenson -- "go their own way."

But Lapham countered, "Merely providing the opportunity to the defendant to act on his own predisposition is not inducement."

Jenson, 22, and Weiner, 21, pleaded guilty and testified against McDavid. They were allowed to plead to lesser charges, and they hope the prosecutors will recommend lenient sentences for them.

U.S. District Judge Morrison E. England Jr. will instruct the jury on the law this morning and the panel will then begin deliberations. McDavid is facing at least five years in prison and not more than 20.

The Bee's Denny Walsh can be reached at (916) 321-1189 or dwalsh@sacbee.com.
Edition: METRO FINAL
Section: METRO
Page: B1

THE BELIEVERS

Anna's "friends" believed in striking a blow against capitalism and for the environment. Anna believed they were dangerous terrorists. Did she lead them down the primrose path to self-destruction, or did she save us from extremists run amok? Maybe not even Anna knows for sure. **By Andrea Todd**

Former FBI informant "Anna" returns to the Nimbus Dam, one of the sites, she says, environmental extremists had considered bombing



It had been a long day at the 2005 CrimethInc Convergence in Bloomington, Indiana, a day of extremes: extreme heat, extreme stress, extreme opinions. Each year since 2002, hundreds of activists—environmental and animal rights radicals, anarcho- and crust-punk bands, tree huggers, vegans, and freegans—descend on urban centers from Athens, Georgia, to Winona, Minnesota, for CrimethInc (a nod to the Orwellian concept of "Thoughtcrime"). The event is a conflagration of protests against all things capitalist and consumerist: record labels, the market economy, corporate influence, working for a living. Food is available in exchange for information (holistic healing, legal advice, propagandist leaflet publishing). No money is allowed; sharing is required. Signs, posted everywhere, announce POLICE NOT WELCOME.

For two years now, a young woman in camo pants, black sweatshirt, military boots, and pink hair, known to both her fellow eco-

activists and FBI employers as "Anna," had been crashing the party. At her first CrimethInc (Des Moines 2004), she'd met 26-year-old Eric McDavid, now seated beside her in her compact car. He'd hit her up for a ride to Chicago rather than make the 230-mile journey via the anarchist-favored mode of transport, train-hopping. Both looked forward to the ride for different reasons. McDavid wanted to spend time alone with this woman he'd met a year earlier, who liked to talk about blowing things up; get to know her better. She wanted to get to know him better too. Just not in the same way.

The car stank of body odor and sweat, thanks to the extremists' rejection of regular bathing and hygiene products like antiperspirant (too many brain-withering chemicals). Vicks VapoRub, which Anna routinely dabbed inside her nose, made it barely tolerable. After a few minutes of idle road-trip banter about the conference and flirtations among their fellow activists, Anna, doing as she'd

Douglas Adreko

been instructed by the FBI, steered the conversation toward a college buddy of McDavid's, Ryan Lewis.

Lewis was an environmental extremist—at that time sitting in the Sacramento County Jail, awaiting his trial on charges of conspiracy to commit arson. Lewis had allegedly planted bombs in office building and housing development sites, crediting ELF—the Earth Liberation Front, a loose network of radical environmentalists—with his work.

"So, did you help him?" Anna asked. He said no, he hadn't.

"I don't believe you—you're pretty militant," she sassed back.

"I have my own plans," McDavid responded, and talked a bit about the bomb recipe he'd scored at Mountain Justice. He asked Anna, whom he knew as a medic in the movement, if he blew his hand off building a bomb, would she take care of him?

"I'd have to think about it."

After a tense silence, McDavid told Anna that if he ever found out she was a cop, he'd kill her.

Anna had a split second to react and get it right. Did he know? Did he suspect? Was it all over?

"Fuck you!" she shouted back, keeping her eyes on the road, feeling her face flush. "You think that about me after all this time? Fuck you! If I find out you're a cop, I'll kill you!"

McDavid smiled and settled back in his seat. "Good," he said.

This is Anna's version of the story (McDavid denies this conversation ever took place), and like so many of her spy tales, it unfolds with cinematic flourish, showcasing her rapid thinking under pressure. Arranging to meet her has been no easy task. She will not tell

that I come from a line of cops and firefighters, she's comfortable with that.

The second time we meet—same place—Anna apologizes for not greeting me right away. She said she thought she'd spotted my car, pointing to another white Honda Civic. "But it wasn't your license plate." She also apologizes for being so paranoid, detailing the threats against her life, via phone, e-mail, and in posts on ELF message boards. "I've just started rebuilding some of the personal relationships I had to let go," she says, including a boyfriend. She had no way to explain to her parents the money she was getting from the FBI—"They thought I was dealing drugs."

Later, the FBI told her that her work was "nothing short of heroic," that they'd placed undercover agents in eco-terrorist cells before, but they had all been found out. Even her bitter enemies admit her sleuthing has rocked the environmental extremist movement.

Some critics dismissed her as "an easily bribed student," but truthfully, money had nothing to do with it. Anna says she grew up "happy" in an upper-middle-class family, the middle child and only girl, who, like the stereotype, yearned for attention. Her father was an educator, her mother a homemaker; both were once what Anna describes not unaffectionately as "former Vietnam-era protest hippies. But that was 35 years ago," she quickly points out. "I wasn't rebelling by adopting moderate conservative views."

As a 15-year-old, Anna says she was so enraged by 9/11 that just days afterward, she e-mailed a site called Militarywomen.org expressing her desire to join the Army and study counterintelligence. "My friends and I saw that plane fly into the World Trade Center, and we thought right away that it was [some Palestinian]

"I had no idea what I was getting into. Here I was, getting knocked to the ground by the NYPD, having an eco-terrorist threaten to kill me. I felt like I was in over my head."

me where she lives; she will come to me, insisting on a public spot in Folsom, California, near Sacramento. As I drive into the lot in front of an area coffee shop, my cell phone rings. "I think you just pulled in," she says. Then, "It's Anna."

I check my rearview mirror. "Where are you?" I ask, but the line's dead. I snap the phone closed, check again, and there she is. These days, she's a brunette. In jeans, a blazer, and makeup, she looks older than I expected (she won't confirm her age, but according to newspaper reports, she'd be about 22 now); still, she has the skin of an adolescent and the creamy, pudgy hands of a child. When she drops her keys and bends to retrieve them, you can spot a colorful tattoo on her back.

Before acquiescing to a face-to-face, she had laid down some ground rules in our e-mail exchanges (which, though her tone is wary and businesslike, are also punctuated with the occasional emoticon): no talk about where she's from, her family, what she studied in college, what she's doing now. As we get to know each other better, as we will over the course of several days, driving her rental car to revisit the sites her cell targeted for bombing, and over wine she orders as expertly as a sommelier, she opens up, then just as quickly changes her mind about what details I can print. She makes many snap judgments: "I heard you went to Berkeley and was like, Oh, no, a hippie." But when she learns

terrorist group," she recalls, adding, "Keep in mind, we were teenagers reading *The Economist*." By 2003, to escape her parents' acrimonious divorce, Anna had left high school, taken the GED, and started college in Miami.

Perhaps, as part of a generation shaped by 9/11, Anna remained attuned to terrorism—any terrorism—on U.S. soil, developing a hatred of those who would kill innocent Americans and a heightened sense of retribution. (While so many of her generation today burn with Obama fever, Anna staunchly supports McCain. "I'm a hawk," she proclaims.) And so when in October 2003 one extremist group claimed responsibility for the ammonium-nitrate bombing of the Pleasanton, California, offices of Shaklee Inc., a maker of personal care products (and which, ironically, has ranked since 1989 on PETA's list of companies that don't test on animals), "It showed me that anyone can be a target," Anna says, darkly. The well-publicized anonymous e-mail explaining the violent act—though damage was minimal—read like a serial killer's, declaring that the size of bombs would be doubled with each attack: "Customers and their families are considered legitimate targets," it read. "...You never know when your house, your car even, might go boom."

Enrolled in a challenging night class (she won't say on what subject), Anna was determined to impress her "brilliant" profes-

sor. Reading in the paper about activists gearing up to protest the Free Trade Area of the Americas Miami conference—the FTAA seeks to unite the North and South American economies, but critics say it exploits underdeveloped countries—she decided to attend some of the meetings for an extra-credit project. On her

police department: “This is really impressive work.” They were saying, “Could you come down here to the Command Center this afternoon and talk about it with us?”

“And I’m like, Who? Huh?”

Anna met with two Miami police officers who wanted to send



If the cellmates succeeded in their plans to implode the Nimbus Dam, U.S. Attorney McGregor Scott claimed, it would have made “what happened in New Orleans after Hurricane Katrina look like a Sunday pancake breakfast.”



(Counterclockwise, from top) The handbook of the now-defunct Black Tea Society, an anarchy group formed to protest the 2004 Democratic National Convention; a family photo of Eric McDavid; Anna (front, second from right) marches to protest the G8 summit in June 2004; United for Peace and Justice protesters rally in front of New York City's Madison Square Garden the day before the 2004 Republican National Convention

first attempt, she was turned away at the door. Anna returned

the next night, this time having dressed in the attire she'd noticed the others wearing: musty, mismatched Goodwill clothing and military boots. She had washed off her habitual mascara and lipstick and wrapped her head in a scarf.

Hanging around the gathering, it was easy for Anna to pick up information about the protestors' plans—from where marches would be held to where the trade talk bigwigs were staying. The following evening she presented her report. The professor wasn't the only one impressed. Afterward, one of her classmates, a Florida highway patrol officer, approached her, asking if he could take home a copy of the report.

“The next morning at 8 A.M., I’m a college student, right? Half-asleep and the phone rings—no shit, I get a call from the Miami

her to the Convergence, an epicenter of activist planning where protestors get information, instructions, supplies. “Law enforcement is easy to spot in these groups,” Anna says. “Cops put the clothes on, but they walk a certain way, they stand a certain way”—it’s the reason for the agency’s failure to penetrate the movement, she claims. “They remained adversarial. I had more of a researcher’s viewpoint.”

Anna’s first assignment would be to attend the G8, or Group of Eight summit, near Atlanta later that summer. An international forum for the governments of the eight nations who represent 65 percent of the world economy and the majority of military expenditure, G8 summits are extremist hot spots. The Miami agents also wanted to book her for both the Democratic and Republican National Conventions, in Boston and New York, respectively, later in the summer. For any investigation of these groups to be legitimate—to get around the “freedom of assembly” right U.S. citizens are afforded—law enforcement needs to have proof of illegal activity. Anna’s FTAA report gave them the green light. “This was Christmas come early for them,” Anna says with a laugh.

Although ELF and its furry-friendly cousin, the Animal Liberation Front (ALF), are intent on destroying government and corporate property without any loss of life—in the roughly 15 years they’ve been organizing, there has been an estimated \$100 million in damage without a single fatality—the Bush administration likens these groups to Al-Qaeda, and considers them “one of the FBI’s highest domestic priorities,” as FBI Director Robert S. Mueller III has said. Under Bush, since 9/11, the number of members in the Bureau’s Joint Terrorism Task Forces (JTTFs) has more than quadrupled. The Feds’ efforts have resulted in several high-profile busts, including “Operation Backfire”—the government’s decade-long investigation and subsequent indictment in 2006 of 11 of the country’s most notorious environmental activists, known as “The Family,” credited for much of the big-damage, “direct-action” eco-terrorism, including the \$12 million torching of a ski resort in Vail. Meanwhile, ELF activists claimed responsibility for the costliest act of eco-extremism on U.S. soil, the \$50 million incineration of an apartment complex under construction in San Diego. Eco-extremists believe that developments like these desecrate the surrounding natural environments. “We must all act our consciousness and inflict economic harm upon all of those who are

McDavid: courtesy of the McDavid family; globe: © Win McNamee/Reuters/Corbis; anti-st. Min. — i. Nam...

responsible for the destruction of the earth and its inhabitants. We encourage others to find a local Earth raper and make them pay for the damages they are inflicting," reads a typical statement from one-time ELF spokesperson Craig Rosebraugh.

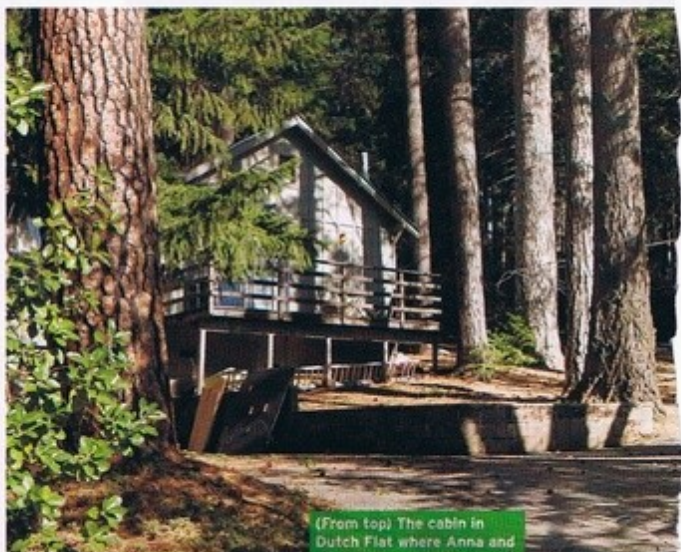
Environmentalists refer to the government's ongoing sweep of these radical groups, many of which have no "list" membership but are composed of a loose network of anarchists and activists, as the "Green Scare," an overt reference to the Red Scare of the McCarthy Era. The stage for the investigation had been set by the broad reach of Bush's Patriot Act and the fact that after 9/11, then-Attorney General John Ashcroft amped up the guidelines for counterintelligence gathering—approving aggressive investigative tactics previously reserved for CIA operations. "The government has it in for a group of individuals they sloppily lump together as anarchists, radicals, ELF and ALF environmentalists—the collective bogeyman," says Ben Rosenfeld, a civil rights attorney in California's Bay Area. "Now they have a slew of new resources and laws to target people for their ideology."

The FBI insists that, because these cells are tightly knit and transient, intensive undercover work, secret surveillance, and aggressive pressure of those arrested and charged with crimes to cooperate, is the only effective way to stop the attacks before they are carried out. Civil liberties groups naturally oppose such tactics in the name of terror-watching. "Calling individuals associated with any of these groups 'the No. 1 threat to security' is really hyperbolic," Rosenfeld says, as FBI Deputy Assistant Director John Lewis did in 2005. Since 1990, more than 1,800 criminal acts in the U.S. have been attributed to ELF, ALF, and similar groups, says FBI spokesperson Bill Carter (but they include everything from vandalism and arson to threatening letters and phone calls). "Basically, the FBI no longer concentrates on crime solving, but has moved to crime prevention"—which creates some serious constitutional issues, namely that innocent-until-proven-guilty cornerstone of our legal system.

Yet, nonviolent environmental groups such as Greenpeace, Earthjustice ("The Earth's lawyers"), and even Earth First!, the original eco-terrorist organization, are quick to distance themselves from these extremist factions. Most contend that eco-terrorists have the same negative effect on the green movement as Muslim terrorists have on the Islamic faith: guilt by association.

"To believe that these people aren't capable of harm or serious attack is not giving them enough credit," Anna says, as we speed along California's Highway 80 in her rental car to the cabin in Dutch Flat, the wooded spot where the group attempted its first homemade bomb. "These people believe in this movement on a very deep and spiritual level.... The earth is feeling the pain of the dying birds and trees, and she is sending out a call to arms, a spiritual and religious call to arms."

But there's no mistaking the typical anarchist/eco-activist gathering for an Al-Qaeda training camp; a three-ring circus is more like it. G8 was no exception, and activists were cooking up big plans. "These people look back to the World Trade Organization riots in 1999 as their big moment: We had the revolution for a little bit," Anna says, referring to the five days during which 50,000 protesters swarmed Seattle, rioting and looting, resulting in 600 arrests. "G8 was supposed to be WTO II." Anna put school on hold in order to throw herself into the planning meetings for G8 and the political conventions—"I thought it would be temporary, like a summer break, and then I'd be right back in school." In the meantime, she had been perfecting her undercover role. Choosing the identity of a medic—one offering the most passivity within the movement—Anna would offer aid or assistance to protesters suffering from hypothermia or heat exhaustion and carry supplies of holistic medicine: lavender bandages, homemade splints, natural



(From top) The cabin in Dutch Flat where Anna and "friends" conspired; one of their targets: the Institute of Forest Genetics, which genetically develops trees

oils and herbs. Her uniform consisted of the camo pants, boots, sweatshirt, red armband, and Palestinian kaffiyeh scarf that help members blend in during protests. An "initiation tattoo"—a skull and black flag on her shoulder—is part of her undercover work as well; she intends to have it removed as soon as she can save the three grand it costs to do so.

Despite organizers' aspirations, only about 50 protesters showed up at G8—though it wasn't a complete loss. As a "confidential source," Anna was providing the agency with names, reports on any illegal activity, and observations about the inner workings of the movement. And it was there that Anna met a quiet young protester called Ollie—"as in Ollie Oxen," Anna says, the phrase used in children's hide-and-seek games and the name of his pro-eco, anarchist website (most serious activists use handles). "Ollie" was actually Zachary Jensen, who lived in Tennessee and was so poor that he qualified for—and helped feed his comrades with—food stamps. Via Jensen and others, Anna scored an invite to the Crime+Inc Convergence in Des Moines, where law enforcement had most wanted to place her. "You are invited to attend these things when you serve a role, are considered trustworthy and important," she says.

In August 2004, Anna phoned Jensen from a Des Moines truck stop to say that she'd just hitchhiked up from Florida, and could someone come and get her? Jensen, accompanied by four friends, piled into a car to pick her up. One of those friends was McDavid.

Eric McDavid grew up in Orangevale, California, a middle-class suburb near Sacramento. Six feet tall and 200 pounds, the affable redhead played football for Casa Robles High School and worked as a carpenter for a bit while studying philosophy and conflict resolution at Sierra College. His parents—mother, a marriage and family therapist; father, a computer engineer—both from midwestern farming families, raised their children with a respect for the land. McDavid had been involved with the peace movement since the beginning of the Iraq war; when his parents gave him *Dude, Where's My Country?*, Michael Moore's anti-Bush policy polemic, it changed his life forever.

Today, seated on the other side of a glass pod in the Sacramento County Jail, McDavid has dropped more than 50 pounds from hunger-striking for vegan food, as a result of which he has also



Douglas Adesko

developed a heart condition. His collarbone juts from his orange jumpsuit. His head is shaved but his goatee is strawberry blond, giving him an incongruously jolly look. He reaches under the slot at the bottom of the glass and his handshake is light and quick. He sits down and smiles. Smiles even when I mention Anna's name.

McDavid reluctantly recalls details of their first meeting. "She had bright pink hair and wore a camouflage skirt," McDavid says. "I was scared of her. She had this strong, feminine energy. Very independent, which I thought to be very cool." The hitchhiking story, he admits, was part of the allure at first. "Now I know, hell no, she didn't hitchhike. I know now the FBI dropped her off." (When I ask Anna about this later, she just laughs.)

"So she arrives and starts throwing her stuff around," McDavid continues, noting that she wasn't exactly spouting activist rhetoric. "She was very subtle about everything."

Almost everything: "I'm out smoking a cigarette and she comes and stands next to me and says, 'So when are you gonna let

without incident, she said." (Meanwhile, Anna was actually sitting in a New York coffee shop being debriefed by the Miami FBI.)

The months following President Bush's reelection in November 2004 ushered in a time of heightened eco-terrorist activity. A series of crude explosive devices was discovered in upscale subdivisions and an apartment complex, all in northwestern California. Graffiti sprayed nearby declared WE WILL WIN—ELF, and letters sent to area papers said more actions were planned. Law enforcement ratcheted up their vigilance, and McDavid dropped out of sight just after investigators arrested his college friend Ryan Lewis on charges of arson. Two weeks later, FBI agents showed up on the McDavid family's doorstep.

The McDavids were puzzled about the inquest, describing their son as a peacemaker and an animal lover who settled squabbles between his two younger sisters, who would scare them with spiders and then transport the spiders, by hand, back to the garden. "He



"Anna is still inside the car and I'm asking myself, Why aren't they worried about her, why are they leaving her alone? And that's when it hit me. That's when I knew."

me go to bed?" McDavid recalls, grinning at the supposed implication. "I look at Jensen, he looks at me, and we're like, Huh. Okay. So she's like that." The two ended up sleeping next to each other, but nothing happened. ("I think our feet touched," Anna recalls emphatically.)

Anna describes her first impression of McDavid as "this chubby kid who played football," "warm to everyone at the gathering," and "a real gentleman." She was aware of her effect on him, though conventional modes of flirtation weren't going to win any points with the opposite sex. "One of the best things about this movement is the way women are treated and viewed," Anna says. "They reject typical standards of beauty, that you have to be stick-thin, with Pantene hair, perfect skin. I was often told if I didn't look so mainstream I'd be more attractive. They focus on a woman's independence, her passion, her conviction. And she is treated as an equal." Furthermore, Anna had fashioned herself into a "straight-edge asexual": "I met a woman early on who had this persona, and I sort of adopted it for myself," she says. "The idea being, my body is a temple. No drugs, no chemicals, nothing will come into my body, not even a penis." Anna thinks it was partly her off-limits identity that continued to fuel McDavid's interest.

And, no doubt, her ability to play the impassioned, balls-out protestor. When the four regrouped later that month on the steps of the New York Public Library for the RNC demonstrations—where AIDS activists protested nude, mothers of soldiers killed in Iraq carried signs that read BUSH KILLED MY SON, and eco-activists arrived with their giant Earth float and Krazy Glue to gum up department store doors—Anna headed for the eye of the storm, even as her comrades hung back. "Anna gets hyped up about moving to the upper platform and tries to recruit the rest of us to do the same," McDavid says. "About five go up, and the cops converge on the whole group." Handcuffed, she was led off to a van parked on the street. "I'm concerned. I'm wondering, Why they hell are they grabbing her?" he says. She never emerged from the van.

Jensen was also bothered by the arrest. "We talked later about how she just—poof!—disappeared. Held for two days, then released

wouldn't let any of us kill spiders," Eileen McDavid says. An open-minded mother, she saw the whole "traveling" period as part of her son's journey to find himself. At one point, Eric had expressed that he was in love with two women (he'd been dating someone from outside the movement) and was trying to decide between them. "He was at that age, so yes, I thought, maybe this is it, maybe he's serious," she shrugs. It saddens her now to realize that one of these women was Anna.

Anna finally laid eyes again on McDavid that summer at the apartment of a friend of Jensen's named Lauren Weiner, "Wren." Brought up in the affluent New York City suburb of Pound Ridge, Weiner was active in the eco-movement while studying at the Philadelphia College of Art. McDavid was "barely recognizable," Anna recalls. "He looked like a Viking. He was lean, buff, like he'd been working out. He had all these piercings and was suddenly so radicalized." At one point, out on Weiner's balcony, McDavid approached Anna: "I want to talk to you in private," he said. McDavid confessed his feelings for her. "He said he thought we were soul twins, we needed to be together. He put his arm around me."

In a later recorded conversation about that night (after Anna's status had been upgraded to wear a wire), she reveals to Weiner that she called out McDavid on how much he'd changed and asked about his influences. "Well, you, for one," he allegedly responded. How much of McDavid's hard-core transformation was an attempt to please Anna, and how much of it was self-directed, would become a pivotal question later on.

Anna and McDavid were together that August at the Bloomington CrimethInc Convergence, at which about 300 people participated in workshops on subjects such as how to maintain a vegan lifestyle, be a political prisoner, or break out of handcuffs ("Master keys for handcuffs," says Anna, adding, "Information from that workshop went out to everyone in the FBI."). At the conference's close, McDavid eagerly hopped that ride with Anna to Chicago, during which Anna says he talked about Lewis, confirming FBI suspicions about their association and leading the agency to tag him as a person of interest.

(CONTINUED ON page 323)

THE BELIEVERS

CONTINUED FROM page 272

At this point, Anna says she was giving serious thought to leaving the FBI. "I had no idea what I was getting into," she says. "Here I was, getting knocked to the ground by the NYPD, thrown in a van, having an eco-terrorist threaten to kill me. I felt like I was in over my head and that no one was watching out for me." The FBI asked her to stay on the job and to focus on McDavid. They also transferred her from Miami to Philly, where she met her handler, Special Agent Ricardo Torres.

She and Torres bonded immediately. "There were other agents there responsible for the investigation," Anna says, "but his job was to keep me alive." She spoke to Torres at least once a day; Torres was impressed by Anna's work and quickly came to trust her. "She was so young, and she wasn't an agent," he says, "but everything she said would happen, happened. I was able to verify every bit of information she passed on to us." Anna, meanwhile, trusted Torres so completely she revealed facts about herself she'd never told anyone: She'd been a victim of sexual assault in college. "Torres was there for me," she remembers. "Toward the end, [he] had arguments with agents about my safety, how far things would go before the whole thing was called off. He was the only one who had my back the whole time." A big reason she stuck with the work, and didn't bail at this point, Anna says, was because of Torres.

McDavid, perhaps feeling rebuffed by Anna, avoided her for the next several months. Claiming he'd hopped the wrong train, he failed to show up at Feral Visions, a green utopian gathering in southeastern Tennessee, where attendees camp out, use compost toilets, forage for food, even start fires by rubbing sticks together. (In one comical episode, Anna saved the day under heavy rain by sneaking in fire-starting sticks bought at Wal-Mart; Weiner hailed her as "the Wilderness Fire-starting Goddess" and passed along news of Anna's prowess to McDavid.) McDavid also failed to invite Anna to a Philadelphia music festival that he attended with Weiner and Jenson. It was at this event, Anna alleges, that Eric discussed plans with the other two to make "big booms" everywhere (Weiner found the word *bombstoo* scary, Anna said). This was seen by the FBI as the first initiation of members into a terrorist "cell." Soon, though, McDavid sent Anna an e-mail pouring out his feelings:

Hey, what's up? Feelin', I don't know, nostalgic, I guess. Feel like writin'. Totally miss you. You're never far from my thoughts or heart. Guess I've been fighting that last part a bit. Okay, a lot. I truly value the time that I've been able to spend with you.... I can still remember your voice, your smile, and that last embrace in Philly. Giggly chills. Don't mean to trip you out. It's just the way I feel, and it feels good to get it out....

Much love, me.

Anna showed the e-mail to agents, who presented her with a seven-page psychological manual on how to handle McDavid. "They said if he makes another advance, what you need to say to him is to calm him, to mollify him, is that we need to put the mission first. There's time for romance later."

Her relationship with McDavid was of constant concern to the FBI; Anna, clearly insulted, conjectures it's because she's female. "I think

they thought I was weak. They kept saying, 'He keeps coming at you,' assuming that I would eventually fold, that I didn't have the balls or the fortitude to resist him. I kept telling [the agents] over and over, 'It's not gonna happen.'"

When a relationship between informant and subject crosses a line into intimacy, it often leads to small deceptions, jeopardizing the necessary transparency with law enforcement. While Anna was able to fend off McDavid's attentions, she admits that she and Weiner became something "like sisters" over the several weeks she spent in Philly. "It made the job a lot harder. She invited me to an art show of hers. She didn't invite anyone in her family, just me, and I went not as an undercover agent but as a friend." On tape, Anna actually asks Weiner if she's "getting cold feet." "And I was sincerely hoping that she would just pull out of it, stay with her family and move back to New York. But she was determined to go," Anna says.

The cell spent Thanksgiving at McDavid's home while his parents were away, discussing their various roles. Weiner was responsible for tactical materials: the equipment, such as a hot plate, stuff for a chemistry lab, and bomb-making books, including *The Poor Man's James Bond*, which she'd bought with her mother's credit card. Jenson's job was to coach the group in "stealthlike ninja tactics," Anna recalls, laughing. "That was his role, to teach us all how to be ninjas." Anna, the medic, was to get medical supplies, easily purchased at Whole Foods.

She was also asked to track down bomb recipes. "I go to the FBI with this, and they said, 'Well, of course we're not going to give you bomb recipes that actually work, so they gave me about half a dozen recipes that were all missing components—something that would smoke and flash.' One of the recipes was similar to Timothy McVeigh's, an ammonium nitrate bomb minus the fertilizer."

Anna searched for a place where they could work and scored a two-bedroom cabin in woodsy Dutch Flat. The FBI paid the rent on the place for the month of January, which she explained away as money she'd earned stripping in college. Collecting the collective in one place presented more of a challenge, however, and after various delays Anna agreed to drive Weiner and Jenson cross-country. The FBI gave her a government-issue '96 Chevy Lumina wired with every high-tech gizmo imaginable (she claimed that her own car had broken down). "They could track me anywhere. They could spot me in a helicopter. That's how seriously the government took this case," Anna says.

Through blizzards and over icy roads, the three drove 20 hours a day. Anna did most of the driving, anxious about allowing Jenson and Weiner to operate the teched-out vehicle, with the recording switch on the driver's side door. During the ride, Jenson and Weiner discussed plans and targets, all of it taped. "They talked about blowing up cell phone towers and a Wal-Mart," Anna insists—conversations that could contradict the notion that she and McDavid were running the show.

The group arrived in Dutch Flat and moved into a cabin wired and ready for surveillance. Cameras and recorders were planted in the home's public spaces—the reason Anna slept out on the couch, in the living area, while the others rotated bedrooms. The FBI set up camp in a trailer a ways down the dirt road, near a volunteer fire station. The cabin was hidden complete-

ly behind the mighty spruces and redwoods. "I had five minutes to save my own life," Anna says, as we walk around the area, thick with dry pine needles that could all too easily catch fire. "And there was snow. The driveway was tricky that time of year."

One afternoon, Weiner called Anna back to one of the bedrooms. "Anna," she sang, happily, "I have something for you...." Anna strolled back to find the three of them grinning. Weiner holding a spider the size of her hand. "Look!" Weiner squealed, shoving it in Anna's face. Deathly afraid of spiders ("And they knew it, too"), Anna let out a scream. The agents could hear it but couldn't see what was happening.

Torres ordered everyone out to the SUVs. He pulled out his gun. "He hears this scream, and he thinks I'm being murdered. He thinks my head is rolling on the floor," Anna says. Without missing a beat, she ran out to the front room, where the cameras would show she was safe, and yelled, "That's the biggest fucking spider I've ever seen!"

It stopped Torres, SUV lights flashing, just in time. Anna admits it was good to know her handlers were on their toes, but had their command station been any closer, the investigation would have been over.

Despite the fact that the group had thus far been short on motivation—Anna admitting on tape that Jenson and Weiner had a tendency to "dillydally" and that the drug of choice among the group was marijuana—the team now "moved fast," Anna says.

Cell phone towers make ideal terror targets because, as noted eco-activist Derrick Jensen, one of McDavid's admitted influences, stated in a well-distributed interview, "You can't make a moral argument for leaving a cell tower up. You aren't going to kill people by taking it out. On the other hand, cell towers kill between five and 50 million migratory songbirds every year." McDavid, Anna says, had also talked up targeting what he called the "Tree Factory," or the Institute of Forest Genetics (IFG), responsible for the genetic development of disease-resistant trees. Allowing the government to manufacture trees would put nature's "real" trees in danger, given their contribution to capitalist growth—and the risk that these alien trees might overtake the native stock.

The group also scouted the Nimbus Dam, which holds back Lake Natoma, a 7,000-acre watershed. Gazing up at the 87-foot-tall, 1,093-foot-wide wall of concrete, the group agreed that, if Nimbus were even a possibility, they'd have to test one of their bombs on concrete first. A lot of it. The dam might have made a good ELF target—because blowing up its gates would actually not result in much death or destruction to the city 24 miles below. Jeff McCracken, a spokesperson for the dam, confirms that the water would just "trickle" down the American and Sacramento Rivers, though U.S. Attorney McGregor Scott would later claim, with much bravado, that thousands of lives had been saved by the FBI's investigation, and that if the cellmates had succeeded in their plans to implode Nimbus it would have made "what happened in New Orleans after Hurricane Katrina look like a Sunday pancake breakfast."

The group set about making bombs in a wooded area beside the cabin. On December 22, Anna's FBI status was elevated further so she could perform OIA, or Otherwise Illegal Activity, and tape the bomb-making sessions. They tried recipes widely available in arsonists' hand-

books—variations on salt and bleach, petroleum jelly and powdered sugar, plumber's putty, battery acid and those trick candles that don't blow out. The standard bomb: a milk jug filled with a gas-soaked rag. Throw in a cigarette until it burns down and catches. *Boom!* "These are the things you fall back on when the sexier bombs don't work," Anna says.

The group bickered over targets and whether to credit ELF with the attack (doing so can carry a higher penalty). The cell members also butted heads over what Anna says McDavid called "collateral damage"—those who die as a result of just being there, in the wrong place at the wrong time. Weiner and Jensen didn't want to risk any fatalities, despite Anna's vocal frustration with their reluctance, the tapes show. McDavid remained silent throughout, until asked his opinion: "Well, if it happens, it happens. It's collateral damage."

A couple of unsettling incidents put already frazzled nerves on edge. On January 11, Anna was pulled over by a California highway patrol officer after rolling through a stop sign on the way to the cabin. "The whole cell was pissed at me," she recalls. "How could you be so stupid, getting pulled over so close to where we are?" they fumed. "The cops will be able to tie us to shit that goes down." The next day, while McDavid was riding shotgun in Anna's car, a recording device tumbled out from under the glove compartment. McDavid picked it up. With typical alacrity, Anna muttered something about the car being a piece of junk, and told him to stuff it back in the glove compartment, which McDavid did. Complicating things, Anna says that during this time, McDavid's interest in her, once seemingly dampened, had picked up.

The infighting culminated in a huge argument the group had that night when a bomb-making experiment fizzled. The tapes clearly present a group on edge. As Anna and Weiner shout over each other, McDavid tries to mediate the situation. Jensen says next to nothing:

M: Take it down a few notches and relax and chill out and maybe come back and chitchat later; that's totally okay.

W: You know, we can all just chill out for the night, like, shit broke down tonight; we, like, stress levels have gone up and fucking down, we've all been tested today, and everyone, I know every single one of our heart rates have been, like, jolted today. Maybe we could all just breathe. I can make pasta.

A: Tomorrow, what were we planning on doing tomorrow? Are we still planning on doing anything tomorrow? Or should I just stop talking about plans?

M: Hmmmm.

W: I would love it if you stopped talking.

A: I would love it if you guys followed a plan! How about that?

When asked about that night, McDavid describes Anna's "meltdown": "She basically had a tizzy fit when the mixture didn't set, kicking at pebbles, yelling, 'Fuck! I'm so fucked!' over and over. Wren and Zach and I are just kind of looking at each other, like, 'What's going on?'" he remembers. "She's flipping out."

He realizes now that, because the project failed, there was no physical evidence of a bomb. And she was running out of time.

After Anna left, "me and Wren smoked a bowl," McDavid recalls. "We needed to take a big time out, see where everyone was when things calmed down." Anna returned from a

two-hour walk, and McDavid suggested that they start fresh the next day, shop for more supplies and try to build something they could test. McDavid offered Anna one of the bedrooms, suggesting that she might feel more relaxed if she had her own space. But Anna insisted on sleeping on the couch for one more night.

Anna had, in fact, left the group to discuss the situation with Torres and the agent in charge of the operation. Arriving at the command center crying and shaking, she insisted she couldn't continue much longer, that the stress level was too high. She reminded the agents about what had happened with the tape recorder that fell into McDavid's hands, and reminded Torres of her history with sexual assault. "I was experiencing some kind of flashback, to being in a situation with a man who wouldn't leave me alone."

Anna was done.

The agents assured her they would make the arrests the following morning.

That night, as Anna slept, she says she was awakened by her cell phone, in her pocket, vibrating against her thigh. Once awake, she later testified she saw McDavid standing over her, waving a knife. "Sorry," she alleges he muttered, and then he returned to bed. Checking her cell phone, the text, a message from Torres, read WAKE UP. She went back to sleep, albeit fretfully.

The next morning, Friday, January 13, the group went shopping for more bomb supplies. McDavid had left the K-Mart with Anna, Jensen and Weiner were still inside the store. "I leaned back on the hood of the car. It was a pretty warm day for January, and I was just chillin', enjoying the sun," McDavid recalls, "and I heard the locks on the door go click, and then click again, locking or unlocking, and locking or unlocking again, I didn't know. Anna had gotten in the car and was on her cell phone."

As Jensen and Weiner approached the car, two black Suburbans and two black SUVs pulled up, surrounding McDavid, and within seconds, men pointing AR-15s, in shirts with JTTF printed across the chests, were shouting. "Get on the ground. Get on the fucking ground. Get on the fucking ground now!"

"Anna is still inside the car and I'm asking myself, Why aren't they worried about her, why are they leaving her alone? And that's when it hit me," McDavid says. "That's when I knew."

McDavid was handcuffed, as were Jensen and Weiner. Pulling McDavid to a standing position, they searched through the pockets of his cargo pants, McDavid realized later, for a handcuff key. Anna remained in the car.

The three were transported in separate squad cars. According to police reports, Jensen asked the agents, "Are you friends of Anna's?"

As news of the arrest spread, ELF and ALF groups rallied to support the cause of all three, running pictures of Anna on their websites and outing her as an informant. But Weiner quickly turned. In exchange for testimony about McDavid, she admitted guilt to a lesser charge of general conspiracy. Six months later, Jensen made the same deal with prosecutors. After they flipped, they were pilloried as snitches—worse than informants, if that's possible—and green groups withdrew all support.

McDavid, meanwhile, spent a year and a half in a 7-by-11-foot cell in solitary confinement awaiting trial on charges of conspiracy to commit arson against government property. He is

surprisingly chipper, given his long isolation, like only those who are sustained by a belief in their moral rectitude can be. He says he never threatened to kill Anna—"I would never hurt anyone"—and denies the knife-wielding incident, as it's come to be called, ever happened. He has asked to take a polygraph, though the results are inadmissible in court. "Anything. You can inject me with that truth serum; that never happened." (The FBI was unable to provide video of the event nor could they find the "hunting knife.") A sticking point with the jury was McDavid's seeming indifference to related fatalities: "When I was discussing 'collateral damage' with the group, that was a philosophical discussion," says McDavid, arguing that he was making the same case for unintentional loss of life in the war for the environment as President Bush has, many times, for the unintentional loss of life in Iraq.

McDavid's attorney, Mark Reichel, who has defended environmental activists before, fought the conspiracy charges based on the term's legal definition (conspiracy must involve at least two individuals, neither of them government agents). He also tried to prove his client was "entrapped"—in effect, goaded and given logistical support by Anna, and otherwise not "predisposed" to carry out the bombings. Anna was violating the law left and right, maintains Reichel. Guidelines for undercover work are clear: Agents cannot lead, push, cajole, or manufacture—"She admitted [she knew] that on the stand," Reichel says. "What about the part on the tape where she says, 'We need to stick to a fucking plan!' What about that?" But, he adds, it's not her fault. "She didn't know what she was doing. This girl, Anna or whatever, she just wanted to do a good job. It was the FBI's responsibility, when they put her to work, to make sure she knew what she was doing, or, if not, assume the risk when you put someone that novice in such a legally complex situation."

Under cross-examination by Reichel, Torres admitted he hadn't read all of the literature on informants; nor could he recall any specifics about the Attorney General's guidelines regarding political protests. (The prosecutorial team insists that Torres read a condensed version of the document—and besides, they're only guidelines, not laws.)

"If this case teaches one lesson," Reichel says, "it's that's we are at the point where the government can say whatever the fuck they want. Do whatever the fuck they want. Whatever the fuck they want."

Still, the jury voted to convict on September 27, 2007, and at press time the three defendants are still awaiting sentencing. Reichel believes the prosecution will ask for the maximum in both cases: 20 years for McDavid, five for Jensen and Weiner. Anna says that Jensen is currently delivering pizza in Washington State and Weiner is living at home with her mother in New York.

Jensen's lawyer did not return calls, but Weiner's attorney (and cousin), Jeff Weiner, expressed reluctance to comment on the case. "She's scared to death of going to prison," he says. "She's a naive girl who got involved in something she shouldn't have, she accepts responsibility for her actions, and she knows what she did is wrong." Still, he continues, there are very troubling issues in the case. "This is as extreme a case of pushing as I've ever seen. This girl, Anna-Lauren was completely enamored of her. She was like the sister she never had. This is a very disturbing case."

McDavid is optimistic about his appeal. "I

won't be here long," he says. As for Anna, "she's got her own karma and it's gonna bite her so big. She's dealing with her own crap. She's gotta live with herself."

Four months after the guilty verdict, juror Diane Bennett was happy to hear from me, she says, "because I've been bothered by this ever since that day." Bennett was so upset by the judgment that she marched right out to local camera crews. "I said the FBI was an embarrassment," she says, as other jurors scrambled to unload similar opinions. "I hope he gets a new trial. I'm not happy with the one he got."

Bennett and most of the other jurors struggled with the entrapment issue but said the judge's instructions were confusing. Bennett says it was clear from the start that acquittal was not an option. "There were several on the jury who simply would not acquit, and said so. Our only choices were a hung jury or a conviction. People were tired," she says. "We wanted to go home." Still, in spite of her regret over the outcome, Bennett credits Anna with tremendous fortitude and smarts. "She was the brains of the whole outfit. The FBI didn't know what they were doing. She was very, very bright, brave, and motivated. I couldn't have the courage to do anything even remotely like this. I can't even imagine the stress."

Since the trial, Anna has consulted for the FBI on agent training, though she no longer works undercover herself—for now. Torres, for his part, says the agency would be lucky to have her back, once she finishes her education—a bachelor's degree is required to be an agent. However, he adds, "I think she wants to move on. Understandable, after what she's been through."

Anna says she'd someday like to be a professor—something in social studies or international relations—and is currently trying to finish school, reestablish relationships with family members and friends, even date. I work my way around to asking her about whether she feels bad about what happened to her one-time "comrades." "I'm a big believer in personal responsibility," she says without hesitation. "People make choices. If you want to protest consumerism, or destruction of the planet, don't drink Coke. Ride your bike. Don't eat meat or wear fur. These people chose to make a bomb and blow up government property, and now they are paying the price for that choice."

But then, in a singular reflective moment after I've told her about McDavid's diminished appearance following his hunger strike, she admits she feels bad for his family. "I would see them in court, and I remember McDavid talking about how close he was with his family. Compared to the rest of us [in the cell], he had it great, family-wise. They're nice people." She knows his parents will pay whatever it costs and do whatever they can do to get their son acquitted. I point out that this is what parents do. She says she knows. "But I still feel bad," she says, her voice trailing off.

Bennett, the juror, tells me that the foreman, a male in his fifties, "teared up" before he had to deliver the verdict. "In my mind, these were just young people who got carried away. People whose hearts were in the right place. I mean," she pauses, "you know, at least someone is trying to take care of our world and our environment."

COVER

Dress, \$7,435, **gloves**, \$695, by Chanel, at select Chanel Boutique nationwide, call 800-550-0005. **Hat** by Stephen Jones Millinery, \$475, visit stephenjonesmillinery.com. **Earrings** by Neil Lane Jewelry, at Neil Lane (L.A.), call 310-275-5015. **Tights** by Fogal, \$43, at Fogal (NYC), call 212-355-3254.

FASHION NINA

Page 98: Chain, \$6,875, **cuff**, \$9,615, by Toby Pomeroy, visit tobypomeroy.com. **Gown, coat** by Go Green Go by 3.1 Phillip Lim, at 3.1 Phillip Lim (NYC), call 212-334-1160. **Clutch** by Diane von Furstenberg, at Diane von Furstenberg (NYC). **Flat** by Repetto x Earnest Sewn, at the Earnest Sewn Co. (NYC), call 212-242-3414. **Pants** by Stella McCartney, at Stella McCartney (NYC). **Page 100: Sets** by Bella Bliss, call 866-846-5295 or visit bellabliss.com. **T-shirt** by Childish Clothing, call 877-5-CHILDISH. **Clog** by Stella McCartney, at Stella McCartney (NYC, L.A.), call 212-255-1556 or visit stellamccartney.com.

ELLE FASHION: THE LOOK

Page 109: Dress, \$15,000, **belt** by Balmain, collection at Jeffrey (NYC), Intermix (NYC). **Sandals** by Giuseppe Zanotti for Balmain, visit giuseppe-zanotti-design.com. **Bangles** by Alexis Bittar, at Alexis Bittar (NYC). **Cuff** by Marni, at Marni (NYC, Costa Mesa, L.A.). **Page 110: Bag** by Fendi, call 800-FENDI-NY. **Slingback** by Christian Louboutin, at Christian Louboutin Boutique nationwide. **Bikini** by GapBody, call 800-GAP-STYLE or visit gapbody.com. **Tank** by 525 America, visit 525america.com.

ELLE FASHION: TRENDS AND ACCESSORIES

Page 112: Bags by Fendi, \$6,030 each, call 800-FENDI-NY. **Watch** by Swatch, at Swatch stores nationwide, call 866-382-4701. **Dress** by Emilio Pucci, visit emiliopucci.com. **Pants** by Balmain, visit intermixonline.com. **Shoe** by Donald J. Pliner, call 888-307-1630. **Bag** by Roger Vivier, \$15,900, call 212-861-5371. **Shoe** by Prada, call 888-977-1900. **Page 114: Bracelet** by Bulgari, at Bulgari stores nationwide, visit bulgari.com. **Shorts** by Lucky Brand Jeans, at Lucky Brand Jeans stores nationwide. **Bra, boy shorts** by Intimissimi, call 800-888-8200 or visit intimissiminet.com. **Top** by Gap, call 800-GAP-STYLE or visit gap.com. **Jumpsuit, tunic** by Roberto Cavalli, at Roberto Cavalli Boutique nationwide or visit robertocavalli.com. **Page 116: Bag** by Fendi, at Fendi Boutique nationwide. **Bag** by Hollywould, at Hollywould (NYC). **Skirt** by Donna Karan Collection, call 866-240-4700. **Dress** by Carolina Herrera, call 212-944-5757. **Page 120: Rings** by House of Holland, call 646-654-0156 or visit sevennewyork.com. **Bag** by Burberry, \$22,000, visit burberry.com. **Skirt** by Harmon, at Oak (Brooklyn), call 718-782-0521 or visit oaknyc.com. **Dress, belt** by D&G, at D&G Boutique (NYC). **Belt** by Etro, at Etro (NYC, Manhasset, NY; Coral Gables, FL; Las Vegas; Beverly Hills), visit etro.it. **Shirt** by Maison Martin Margiela, call 949-497-1212 or visit anastasiausa.net. **Page 122: Necklace** by Louis Vuitton, \$10,570, call 866-VUITTON. **Page 124: Bag** by Fendi, at Fendi Boutique nationwide. **Page 126: Wedge** by Fendi, at Fendi Boutique nationwide. **Bag** by Roger Vivier, \$7,300, call 212-861-5371. **Clutch** by Stella McCartney, at Stella McCartney (NYC; West Hollywood, CA), call 212-255-1556. **Page 128: Ring** by Suzanne Felsen, \$5,900, at Suzanne Felsen (L.A.), call 323-653-5400. **White gold watch**, \$98,000, **rose gold watch**, \$13,500, by IWC, call 800-432-

9330. **Pendant** by Cathy Waterman, \$19,650, visit twistonline.com. **Bowl** by Michael Aram, call 866-792-ARAM or visit michaelaram.com.

ELLE SHOPS

Page 141: Cuff by John Hardy, call 888-838-3022. **Skirt** by Etro, at Etro (NYC, Manhasset, NY; Coral Gables, FL; Las Vegas; Beverly Hills), call 212-317-9096. **Sandals** by Cesare Paciotti, at Cesare Paciotti (NYC, L.A.), call 310-273-3220 or visit cesare-paciotti.us. **Bag** by Fendi, at Fendi Boutique nationwide. **Brooches** by Tiffany & Co., at Tiffany & Co. nationwide. **Page 144: Dress** by Lanvin, \$17,625, at Barneys New York. **Sandals** by Sigerson Morrison, call 212-219-3893 or visit sigersonmorrison.com. **Necklace** by Josh Hickey, visit joshhickey.com. **Page 146: Bracelets** by Tous, at Tous stores nationwide. **Boot** by Jimmy Choo, call 866-J-CHOO-US. **Bag** by Chanel, call 800-550-0005. **Vest** by Emilio Pucci, at Emilio Pucci stores nationwide. **Page 150: Shirt** by Undercover, at Susan (San Francisco, Burlingame, CA), call 650-347-0452. **Shirt** by Etro, at Etro (NYC, Manhasset, NY; Coral Gables, FL; Las Vegas; Beverly Hills), call 212-317-9096. **Bikini** by Shay Todd, call 323-655-3760 or visit shaytodd.com. **Pins** by Giorgio Armani, call 212-988-9191. **Tote** by Old Navy, call 800-OLD-NAVY or visit oldnavy.com. **Key ring** by Mulberry, at Mulberry (NYC, Manhasset, NY; Atlantic City; L.A.), call 888-685-6856. **Trousers** by Diesel, at Diesel (NYC, L.A.), call 877-433-4373 or visit diesel.com. **Page 152: Dress** by Old Navy, at Old Navy stores nationwide, call 800-OLD-NAVY. **Ring** by John Hardy, visit johnhardy.com. **Bag** by Escada, call 800-869-8424 or visit escada.com. **Sandal** by L'Autre Chose, at the Shoe Box (Plainview, NY), call 516-931-7775 or visit shopheshoebox.com. **Bag** by True Religion, at True Religion Brand Jeans stores nationwide, call 866-427-1119. **Page 156: Cuffs** by Marni, at Marni (NYC; Costa Mesa, L.A.), visit marni.com. **Skirt** by Dries van Noten, similar styles at Jeffrey (NYC). **Sandal** by Sergio Rossi, at Sergio Rossi (NYC), call 212-956-3304 or visit sergirossi.com. **Tote** by Salvatore Ferragamo, call 800-628-8916. **Page 158: Bag** by Roger Vivier, \$9,100, call 212-861-5371. **Bikini** by Araks, call 212-473-2478 or visit thelittleleft.com. **Wedge** by Giuseppe Zanotti Design, at Giuseppe Zanotti Design Boutique (NYC; Costa Mesa, CA), call 714-979-3300 or visit giuseppezanotti-design.com. **Top, dress, belts** by Alessandro Dell'Acqua, at Alessandro Dell'Acqua Boutique (NYC), call 212-253-6861. **Top** by Koi Suenamagat, collection at Wendy Foster (Santa Barbara, CA), call 805-565-1506 or visit wendyfoster.com. **Wedge** by Giorgio Armani, at Giorgio Armani Boutique nationwide or call 212-988-9191. **Page 160: Bag** by Giorgio Armani, \$7,995, call 212-988-9191. **Gown** by Diane von Furstenberg, call 646-486-4800. **Earrings** by H.Stern, \$5,400, call 800-7-H-STERN or visit hstern.net. **Bag** by Hollywould, at Hollywould (NYC). **Bikini** by Pitahaya Swimsuits, visit vogueette.com. **Swimsuit** by Emilio Pucci, visit emiliopucci.com.

BURNING UP

Page 279: Blazer by Nathan Jenden, visit nathanjenden.com. **Bra** by Deborah Marquit, at Deborah Marquit (NYC), call 212-478-3092 or visit deborahmarquit.com. **Jeans** by J Brand, visit jbrandjeans.com. **Hat** by Stephen Jones Millinery, visit stephenjonesmillinery.com. **Necklace, ring** by Neil Lane Jewelry, at Neil Lane (L.A.), call 310-275-5015.



INCITE! Women of Color Against Violence

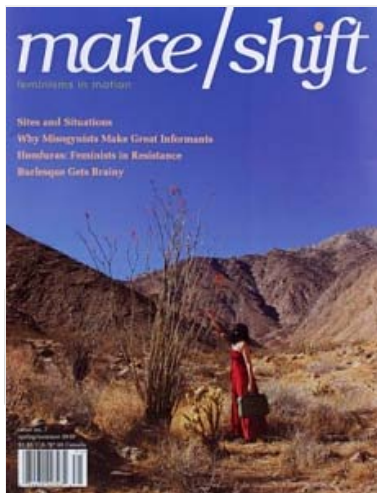
Home Commenting Send news to the INCITE! blog!

Why Misogynists Make Great Informants: How Gender Violence on the Left Enables State Violence in Radical Movements

JULY 15, 2010

by inciteblog

tags: community accountability, feminism, law enforcement violence, state violence, women of color



Originally published in *make/shift* magazine

Some people may have seen this article already, which has been making its rounds on Facebook and the blogosphere, but INCITE! blog editors loved it so much that we wanted to share it here. The piece was originally published in **make/shift** magazine's Spring/Summer 2010 issue and written by **Courtney Desiree Morris**.

42
tweets
retweet

In January 2009, activists in Austin, Texas, learned that one of their own, a white activist named Brandon Darby, had infiltrated groups protesting the Republican National Convention (RNC) as an FBI informant. Darby later admitted to wearing recording devices at planning meetings and during the convention. He testified on behalf of the government in the February 2009 trial of two Texas activists who were arrested at the RNC on charges of

making and possessing Molotov cocktails, after Darby encouraged them to do so. The two young men, David McKay and Bradley Crowder, each faced up to fifteen years in prison. Crowder accepted a plea bargain to serve three years in a federal prison; under pressure from federal prosecutors, McKay also pled guilty to being in possession of "unregistered Molotov cocktails" and was sentenced to four years in prison. Information gathered by Darby may also have contributed to the case against the RNC 8, activists from around the country charged with "conspiracy to riot and conspiracy to damage property in the furtherance of terrorism." Austin activists were particularly stunned by the revelation that Darby had served as an informant because he had been a part of various leftist projects and was a leader at Common Ground Relief, a New Orleans-based organization committed to meeting the short-term needs of community members displaced by natural disasters in the Gulf Coast region and dedicated to rebuilding the region and ensuring Katrina evacuees' right to return.

I was surprised but not shocked by this news. I had learned as an undergrad at the University of Texas that the campus police department routinely placed plainclothes police officers in the

ABOUT INCITE!



INCITE! Women of Color Against Violence is a national activist organization of radical feminists of color advancing a movement to end violence against women of color and our communities through direct action, critical dialogue, and grassroots organizing. For more info, please visit: <http://incite-national.org>

Connect with INCITE! on facebook!

Follow INCITE! on twitter!

SUBSCRIBE TO RSS FEED

➤ RSS - Posts

➤ RSS - Comments

SEARCH

RECENT POSTS

- 'Women's Rights' in Canada in the Age of Border Control, Imperialism, and Colonialism
- Call for Submissions: Trans Justice and AIDS Activism Zine
- Decriminalization of sex work and Indigenous youth and communities – Response from the Native Youth Sexual Health Network
- Unforgotten Faces – Acknowledging Black Womyn of South Africa
- Take Action Against State Violence

meetings of radical student groups—you know, just to keep an eye on them. That was in fall 2001. We saw the creation of the Department of Homeland Security, watched a cowboy president wage war on terror, and, in the middle of it all, tried to figure out what we could do to challenge the fascist state transformations taking place before our eyes. At the time, however, it seemed silly that there were cops in our meetings—we weren't the Panthers or the Brown Berets or even some of the rowdier direct-action anti-globalization activists on campus (although we admired them all); we were just young people who didn't believe war was the best response to the 9/11 attacks. But it wasn't silly; the FBI does not dismiss political work. Any organization, be it large or small, can provoke the scrutiny of the state. Perhaps your organization poses a large threat, or maybe you're small now but one day you'll grow up and be too big to rein in. The state usually opts to kill the movement before it grows.

And informants and provocateurs are the state's hired gunmen. Government agencies pick people that no one will notice. Often it's impossible to prove that they're informants because they appear to be completely dedicated to social justice. They establish intimate relationships with activists, becoming friends and lovers, often serving in leadership roles in organizations. A cursory reading of the literature on social movements and organizations in the 1960s and 1970s reveals this fact. The leadership of the American Indian Movement was rife with informants; it is suspected that informants were also largely responsible for the downfall of the Black Panther Party, and the same can be surmised about the antiwar movement of the 1960s and 1970s. Not surprisingly, these movements that were toppled by informants and provocateurs were also sites where women and queer activists often experienced intense gender violence, as the autobiographies of activists such as Assata Shakur, Elaine Brown, and Roxanne Dunbar-Ortiz demonstrate.

Maybe it isn't that informants are difficult to spot but rather that we have collectively ignored the signs that give them away. To save our movements, we need to come to terms with the connections between gender violence, male privilege, and the strategies that informants (and people who just act like them) use to destabilize radical movements. Time and again heterosexual men in radical movements have been allowed to assert their privilege and subordinate others. Despite all that we say to the contrary, the fact is that radical social movements and organizations in the United States have refused to seriously address gender violence [1] as a threat to the survival of our struggles. We've treated misogyny, homophobia, and heterosexism as lesser evils—secondary issues—that will eventually take care of themselves or fade into the background once the “real” issues—racism, the police, class inequality, U.S. wars of aggression—are resolved. There are serious consequences for choosing ignorance. Misogyny and homophobia are central to the reproduction of violence in radical activist communities. Scratch a misogynist and you'll find a homophobe. Scratch a little deeper and you might find the makings of a future informant (or someone who just destabilizes movements like informants do).

The Makings of an Informant: Brandon Darby and Common Ground

On Democracy Now! Malik Rahim, former Black Panther and cofounder of Common Ground in New Orleans, spoke about how devastated he was by Darby's revelation that he was an FBI informant. Several times he stated that his heart had been broken. He especially lamented all of the “young ladies” who left Common Ground as a result of Darby's domineering, aggressive style of organizing. And when those “young ladies” complained? Well, their concerns likely fell on sympathetic but ultimately unresponsive ears—everything may have been true, and after the fact everyone admits how disruptive Darby was, quick to suggest violent, ill-conceived direct-action schemes that endangered everyone he worked with. There were even claims of Darby sexually assaulting female organizers at Common Ground and in general being dismissive of women working in the organization. [2] Darby created conflict in all of the organizations he worked with, yet people were hesitant to hold him accountable because of his history and reputation as an organizer and his “dedication” to “the work.” People continued to defend him until he outed himself as an FBI informant. Even Rahim, for all of his guilt and angst, chose to

Against Immigrant Families

RECENT COMMENTS



Sex Work, Migration ... on Sex Work, Migration and Anti-T...



Jeannette on Reflections from Detroit: Tran...

Tweeting Revolution ... on Women in India Use Media, Self...



Che on Call for Submissions: Trans Ju...



vikki on Call for Submissions: Trans Ju...

CATEGORIES

- » Art & Performance
- » Calls for Volunteers/Activists/Job Applicants
- » Calls for Writing/Artistic/Workshop Submissions
- » Events
- » General News
- » Guest Post
- » INCITE! Announcements
- » Language & Action
- » Reflections from Detroit
- » Take Action!

TAGS

Afghanistan Africa **art** BDS movement
Black women body politics campus
organizing Canada Chican@s/Latin@s
community
accountability
community
organizing conference
disability justice disaster
economic justice environmental
justice feminism gender
justice Haiti healing/health justice
immigration justice

leave Darby in charge of Common Ground although every time there was conflict in the organization it seemed to involve Darby.

Maybe if organizers made collective accountability around gender violence a central part of our practices we could neutralize people who are working on behalf of the state to undermine our struggles. I'm not talking about witch hunts; I'm talking about organizing in such a way that we nip a potential Brandon Darby in the bud before he can hurt more people. Informants are hard to spot, but my guess is that where there is smoke there is fire, and someone who creates chaos wherever he goes is either an informant or an irresponsible, unaccountable time bomb who can be unintentionally as effective at undermining social-justice organizing as an informant. Ultimately they both do the work of the state and need to be held accountable.

A Brief Historical Reflection on Gender Violence in Radical Movements

Reflecting on the radical organizations and social movements of the 1960s and 1970s provides an important historical context for this discussion. Memoirs by women who were actively involved in these struggles reveal the pervasiveness of tolerance (and in some cases advocacy) of gender violence. Angela Davis, Assata Shakur, and Elaine Brown, each at different points in their experiences organizing with the Black Panther Party (BPP), cited sexism and the exploitation of women (and their organizing labor) in the BPP as one of their primary reasons for either leaving the group (in the cases of Brown and Shakur) or refusing to ever formally join (in Davis's case). Although women were often expected to make significant personal sacrifices to support the movement, when women found themselves victimized by male comrades there was no support for them or channels to seek redress. Whether it was BPP organizers ignoring the fact that Eldridge Cleaver beat his wife, noted activist Kathleen Cleaver, men coercing women into sex, or just men treating women organizers as subordinated sexual playthings, the BPP and similar organizations tended not to take seriously the corrosive effects of gender violence on liberation struggle. In many ways, Elaine Brown's autobiography, *A Taste of Power: A Black Woman's Story*, has gone the furthest in laying bare the ugly realities of misogyny in the movement and the various ways in which both men and women reproduced and reinforced male privilege and gender violence in these organizations. Her experience as the only woman to ever lead the BPP did not exempt her from the brutal misogyny of the organization. She recounts being assaulted by various male comrades (including Huey Newton) as well as being beaten and terrorized by Eldridge Cleaver, who threatened to "bury her in Algeria" during a delegation to China. Her biography demonstrates more explicitly than either Davis's or Shakur's how the masculinist posturing of the BPP (and by extension many radical organizations at the time) created a culture of violence and misogyny that ultimately proved to be the organization's undoing.

These narratives demystify the legacy of gender violence of the very organizations that many of us look up to. They demonstrate how misogyny was normalized in these spaces, dismissed as "personal" or not as important as the more serious struggles against racism or class inequality. Gender violence has historically been deeply entrenched in the political practices of the Left and constituted one of the greatest (if largely unacknowledged) threats to the survival of these organizations. However, if we pay attention to the work of Davis, Shakur, Brown, and others, we can avoid the mistakes of the past and create different kinds of political community.

The Racial Politics of Gender Violence

Race further complicates the ways in which gender violence unfolds in our communities. In "Looking for Common Ground: Relief Work in Post-Katrina New Orleans as an American Parable of Race and Gender Violence," Rachel Luft explores the disturbing pattern of sexual assault against white female volunteers by white male volunteers doing rebuilding work in the Upper Ninth Ward in 2006. She points out how Common Ground failed to address white men's assaults on their co-organizers and instead shifted the blame to the surrounding Black community, warning white women activists that they needed to be careful because New Orleans was a dangerous place. Ultimately it proved easier to criminalize Black men from the

Indigenous women

Islamophobia Latinas law

enforcement violence

LGBT/Queer media

mothering movement building

Muslim women Native American

Palestine reproductive

justice self-care sex trade /
sex work sexual violence

spirituality survival testimonios

transnational transphobia USSF

war women of color
young people

LINKS

- Boarding School Healing Project
- Boycott, Divestment, Sanctions (BDS)
- Center for Immigrant Families (NYC)
- Communities Against Rape and Abuse (CARA – Seattle, WA)
- Creative Interventions (Oakland, CA)
- Females United for Action (FUFA – Chicago, IL)
- INCITE! Local Chapters and Affiliates
- INCITE! Women of Color Against Violence
- Latina Mami (Austin, TX)
- Women's Health and Justice Initiative (New Orleans, LA)
- Young Women United (Albuquerque, NM)
- Young Women's Empowerment Project (YWEP – Chicago, IL)

neighborhood than to acknowledge that white women and transgender organizers were most likely to be assaulted by white men they worked with. In one case, a white male volunteer was turned over to the police only after he sexually assaulted at least three women in one week. The privilege that white men enjoyed in Common Ground, an organization ostensibly committed to racial justice, meant that they could be violent toward women and queer activists, enact destructive behaviors that undermined the organization's work, and know that the movement would not hold them accountable in the same way that it did Black men in the community where they worked.

Of course, male privilege is not uniform—white men and men of color are unequal participants in and beneficiaries of patriarchy although they both can and do reproduce gender violence. This disparity in the distribution of patriarchy's benefits is not lost on women and queer organizers when we attempt to confront men of color who enact gender violence in our communities. We often worry about reproducing particular kinds of racist violence that disproportionately target men of color. We are understandably loath to call the police, involve the state in any way, or place men of color at the mercy of a historically racist criminal (in)justice system; yet our communities (political and otherwise) often do not step up to demand justice on our behalf. We don't feel comfortable talking to therapists who just reaffirm stereotypes about how fucked-up and exceptionally violent our home communities are. The Left often offers even less support. Our victimization is unfortunate, problematic, but ultimately less important to "the work" than the men of all races who reproduce gender violence in our communities.

Encountering Misogyny on the Left: A Personal Reflection

In the first community group I was actively involved in, I encountered a level of misogyny that I would never have imagined existed in what was supposed to be a radical-people-of-color organization. I was sexually/romantically involved with an older Chicano activist in the group. I was nineteen, an inexperienced young Black activist; he was thirty. He asked me to keep our relationship a secret, and I reluctantly agreed. Later, after he ended the relationship and I was reeling from depression, I discovered that he had been sleeping with at least two other women while we were together. One of them was a friend of mine, another young woman we organized with. Unaware of the nature of our relationship, which he had failed to disclose to her, she slept with him until he disappeared, refusing to answer her calls or explain the abrupt end of their relationship. She and I, after sharing our experiences, began to trade stories with other women who knew and had organized with this man.

We heard of the women who had left a Chicana/o student group and never came back after his lies and secrets blew up while the group was participating in a Zapatista action in Mexico City. The queer, radical, white organizer who left Austin to get away from his abuse. Another white woman, a social worker who thought they might get married only to come to his apartment one evening and find me there. And then there were the ones that came after me. I always wondered if they knew who he really was. The women he dated were amazing, beautiful, kick-ass, radical women that he used as shields to get himself into places he knew would never be open to such a misogynist. I mean, if that cool woman who worked in Chiapas, spoke Spanish, and worked with undocumented immigrants was dating him, he must be down, right? Wrong.

But his misogyny didn't end there; it was also reflected in his style of organizing. In meetings he always spoke the loudest and longest, using academic jargon that made any discussion excruciatingly more complex than necessary. The academic-speak intimidated people less educated than him because he seemed to know more about radical politics than anyone else. He would talk down to other men in the group, especially those he perceived to be less intelligent than him, which was basically everybody. Then he'd switch gears, apologize for dominating the space, and acknowledge his need to check his male privilege. Ironically, when people did attempt to call him out on his shit, he would feign ignorance—what could they mean, saying that his behavior was masculinist and sexist? He'd complain of being infantilized, refusing to see how he infantilized people all the time. The fact that he was a man of color who could talk a

good game about racism and racial-justice struggles masked his abusive behaviors in both radical organizations and his personal relationships. As one of his former partners shared with me, “His radical race analysis allowed people (mostly men but occasionally women as well) to forgive him for being dominating and abusive in his relationships. Womyn had to check their critique of his behavior at the door, lest we lose a man of color in the movement.” One of the reasons it is so difficult to hold men of color accountable for reproducing gender violence is that women of color and white activists continue to be invested in the idea that men of color have it harder than anyone else. How do you hold someone accountable when you believe he is target number one for the state?

Unfortunately he wasn’t the only man like this I encountered in radical spaces—just one of the smarter ones. Reviewing old e-mails, I am shocked at the number of e-mails from men I organized with that were abusive in tone and content, how easily they would talk down to others for minor mistakes. I am more surprised at my meek, diplomatic responses—like an abuse survivor—as I attempted to placate compañeros who saw nothing wrong with yelling at their partners, friends, and other organizers. There were men like this in various organizations I worked with. The one who called his girlfriend a bitch in front of a group of youth of color during a summer encuentro we were hosting. The one who sexually harassed a queer Chicana couple during a trip to México, trying to pressure them into a threesome. The guys who said they would complete a task, didn’t do it, brushed off their compañeras’ demands for accountability, let those women take over the task, and when it was finished took all the credit for someone else’s hard work. The graduate student who hit his partner—and everyone knew he’d done it, but whenever anyone asked, people would just look ashamed and embarrassed and mumble, “It’s complicated.” The ones who constantly demeaned queer folks, even people they organized with. Especially the one who thought it would be a revolutionary act to “kill all these faggots, these niggas on the down low, who are fucking up our children, fucking up our homes, fucking up our world, and fucking up our lives!” The one who would shout you down in a meeting or tell you that you couldn’t be a feminist because you were too pretty. Or the one who thought homosexuality was a disease from Europe.

Yeah, that guy.

Most of those guys probably weren’t informants. Which is a pity because it means they are not getting paid a dime for all the destructive work they do. We might think of these misogynists as inadvertent agents of the state. Regardless of whether they are actually informants or not, the work that they do supports the state’s ongoing campaign of terror against social movements and the people who create them. When queer organizers are humiliated and their political struggles sidelined, that is part of an ongoing state project of violence against radicals. When women are knowingly given STIs, physically abused, dismissed in meetings, pushed aside, and forced out of radical organizing spaces while our allies defend known misogynists, organizers collude in the state’s efforts to destroy us.

The state has already understood a fact that the Left has struggled to accept: misogynists make great informants. Before or regardless of whether they are ever recruited by the state to disrupt a movement or destabilize an organization, they’ve likely become well versed in practices of disruptive behavior. They require almost no training and can start the work immediately. What’s more paralyzing to our work than when women and/or queer folks leave our movements because they have been repeatedly lied to, humiliated, physically/verbally/emotionally/sexually abused? Or when you have to postpone conversations about the work so that you can devote group meetings to addressing an individual member’s most recent offense? Or when that person spreads misinformation, creating confusion and friction among radical groups? Nothing slows down movement building like a misogynist.

What the FBI gets is that when there are people in activist spaces who are committed to taking power and who understand power as domination, our movements will never realize their potential to remake this world. If our energies are absorbed recuperating from the messes that informants (and people who just act like them) create, we will never be able to focus on the real

work of getting free and building the kinds of life-affirming, people-centered communities that we want to live in. To paraphrase bell hooks, where there is a will to dominate there can be no justice, because we will inevitably continue reproducing the same kinds of injustice we claim to be struggling against. It is time for our movements to undergo a radical change from the inside out.

Looking Forward: Creating Gender Justice in our Movements

Radical movements cannot afford the destruction that gender violence creates. If we underestimate the political implications of patriarchal behaviors in our communities, the work will not survive.

Lately I've been turning to the work of queers/feminists of color to think through how to challenge these behaviors in our movements. I've been reading the autobiographies of women who lived through the chaos of social movements debilitated by machismo. I'm revisiting the work of bell hooks, Roxanne Dunbar-Ortiz, Toni Cade Bambara, Alice Walker, Audre Lorde, Gioconda Belli, Margaret Randall, Elaine Brown, Pearl Cleage, Ntozake Shange, and Gloria Anzaldúa to see how other women negotiated gender violence in these spaces and to problematize neat or easy answers about how violence is reproduced in our communities. Newer work by radical feminists of color has also been incredibly helpful, especially the zine *Revolution Starts at Home: Confronting Partner Abuse in Activist Communities*, edited by Ching-In Chen, Dulani, and Leah Lakshmi Piepzna-Samarasinha.

But there are many resources for confronting this dilemma beyond books. The simple act of speaking and sharing our truths is one of the most powerful tools we have. I've been speaking to my elders, older women of color in struggle who have experienced the things I'm struggling against, and swapping survival stories with other women. In summer 2008 I began doing workshops on ending misogyny and building collective forms of accountability with Cristina Tzintzún, an Austin-based labor organizer and author of the essay "Killing Misogyny: A Personal Story of Love, Violence, and Strategies for Survival." We have also begun the even more liberating practice of naming our experiences publicly and calling on our communities to address what we and so many others have experienced.

Dismantling misogyny cannot be work that only women do. We all must do the work because the survival of our movements depends on it. Until we make radical feminist and queer political ethics that directly challenge heteropatriarchal forms of organizing central to our political practice, radical movements will continue to be devastated by the antics of Brandon Darbys (and folks who aren't informants but just act like them). A queer, radical, feminist ethic of accountability would challenge us to recognize how gender violence is reproduced in our communities, relationships, and organizing practices. Although there are many ways to do this, I want to suggest that there are three key steps that we can take to begin. First, we must support women and queer people in our movements who have experienced interpersonal violence and engage in a collective process of healing. Second, we must initiate a collective dialogue about how we want our communities to look and how to make them safe for everyone. Third, we must develop a model for collective accountability that truly treats the personal as political and helps us to begin practicing justice in our communities. When we allow women/queer organizers to leave activist spaces and protect people whose violence provoked their departure, we are saying we value these de facto state agents who disrupt the work more than we value people whose labor builds and sustains movements.

As angry as gender violence on the Left makes me, I am hopeful. I believe we have the capacity to change and create more justice in our movements. We don't have to start witch hunts to reveal misogynists and informants. They out themselves every time they refuse to apologize, take ownership of their actions, start conflicts and refuse to work them out through consensus, mistreat their compañer@s. We don't have to look for them, but when we are presented with their destructive behaviors we have to hold them accountable. Our strategies don't have to be punitive; people are entitled to their mistakes. But we should expect that people will own those

actions and not allow them to become a pattern.

We have a right to be angry when the communities we build that are supposed to be the model for a better, more just world harbor the same kinds of antiequeer, antiwoman, racist violence that pervades society. As radical organizers we must hold each other accountable and not enable misogynists to assert so much power in these spaces. Not allow them to be the faces, voices, and leaders of these movements. Not allow them to rape a compañera and then be on the fucking five o' clock news. In Brandon Darby's case, even if no one suspected he was an informant, his domineering and macho behavior should have been all that was needed to call his leadership into question. By not allowing misogyny to take root in our communities and movements, we not only protect ourselves from the efforts of the state to destroy our work but also create stronger movements that cannot be destroyed from within.

[1] I use the term gender violence to refer to the ways in which homophobia and misogyny are rooted in heteronormative understandings of gender identity and gender roles. Heterosexism not only polices non-normative sexualities but also reproduces normative gender roles and identities that reinforce the logic of patriarchy and male privilege.

[2] I learned this from informal conversations with women who had organized with Darby in Austin and New Orleans while participating in the Austin Informants Working Group, which was formed by people who had worked with Darby and were stunned by his revelation that he was an FBI informant.

Article published courtesy of **make/shift magazine** and Courtney Desiree Morris. For more of the author's work visit: <http://creolemaroon.blogspot.com/>.



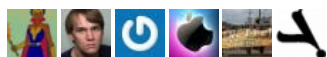
Share this:  **13**

from → Guest Post

← SISTERSONG, SPARK, and SisterLove Defeat SB 529

Reflections from Detroit: 12th Annual Allied Media Conference Report Back →

6 bloggers like this post



 **50 Comments** [leave one →](#)



EnCee [PERMALINK](#)

July 16, 2010 12:01 am

This article is great. Hands down one of the best critiques I have read in a while. I just think it's so sad that so many great activists had to through this type of stuff. Reading about inspiring activists like Angela Davis, Assata Shakur, Roxanne Dunbar-Ortiz, Alice Walker, Audre Lorde, bell hooks, Margaret Randall, Elaine Brown, and Gloria Anzaldúa and knowing they had to go though these types of things just make me wonder what the hell type of movement people are trying to build nowadays. It's like people have learned nothing from the past. I was previously in a Marxist grouping and I think maybe that's why some people in the the leadership, were always so dismissive of feminism and its critical theory.

Review Session 1:

Revisit the following questions:

- a- Answer Schneier's five questions as they relate to your organization: What assets are you trying to protect? What are the risks to these assets? How well does the security solution mitigate those risks? What other risks does the security solution cause? What costs and trade-offs does the security solution impose?
- b- Re-read Eveleigh's instructions for recruiting informers (from Lawrence, pages 20-1). How could resistance groups guard against this?
- c- Consider Williams' conclusions. What lessons does he offer for social movements? Do you agree? How does his perspective relate to the work of your organization?
- d- Describe the relationship between "good politics" and good security. How does this operate at the movement, (internal) organizational, and individual levels?

Review Session 2:

Part One:

The following scenarios and discussion questions are deliberately open-ended. Select four, and discuss for a total of one hour:

Exercise 1: Think of a legal but controversial political campaign that your group is, has been, or might become involved in. Imagine you're organizing a press conference to announce this project.

Brainstorm security concerns. Then brainstorm countermeasures.

Exercise 2: Without discussing it, have each member write out a definition of security. When everyone is done, compare and discuss.

Exercise 3: You're at a national meeting in an unfamiliar city. After the meeting, many members of the organization are at a neighborhood bar and the locals, noticing a large group of strange faces, become inquisitive. One asks you, in a friendly way, about the group you're with, whether you're from out of town. How do you respond? What risks exist here?

Exercise 4: Several members of your group are traveling to a political conference in another country. At the border, you're separated and questioned. During questioning, the border guards take your phones, leave the room, and then return with them several minutes later. After half an hour, they return your phone and allow you to proceed.

How should you prepare for border-crossings? How should you respond to such questioning? What should you do after such questioning?

Exercise 5: Imagine you're a union official and your members have been on strike for months. You launch an ambitious plan calling on thousands of your allies to blockade the port. The local police call you saying they have information that anarchists are planning on coming to the rally and bombing the port. The police want you to cancel. What are the risks each way? What precautions are reasonable?

Exercise 6: You are part of a team of street medics, and you hear that another medic team includes a member who moved to town after being accused of raping several women in another city. What do you do?

Exercise 7: You are at a demonstration against the President, who is scheduled to give a speech. The crowd has been in the street outside the venue for most of an hour, and the president is about 20 minutes late. Then, an activist you recognize gets on the bullhorn and announces that you've won, and the president has canceled his speech. What do you do?

Exercise 8: You're a union organizer, and you're launching an organizing campaign. You plan on fliering at the factory gates to make contact with the workers. Unexpectedly, you get a call from the cops. They've heard you're planning an action, and ask what you have planned. What do you do?

Exercise 9: You've been working in a coalition against police surveillance. The coalition is tenuous at best, with sharp ideological differences, personal acrimony, and power struggles. You hear that one of your rivals is spreading false rumors about you. How do you respond?

Exercise 10: You're in a small organization with several volunteers and one staff member. One of the volunteers begins sexually harassing the women in the group, and is asked to leave. He then proceeds to stalk the staff and make threats against various volunteers. The staff member wants to get a restraining order. What are the costs and benefits? What other options are there? Are there bigger organizational problems that this points to?

Review Session Two, Part Two:

Spend one hour to do both of the following exercises:

Exercise 11: Name a security problem your group has experienced. Evaluate your response. Did you detect the attack quickly? Were you able to learn how and why it happened? Were you able to take corrective action before more harm was done? How was the issue addressed? Were the efforts to address those problems successful? Did they create any other problems, or carry associated costs? Did you identify and fix the weaknesses that allowed the attack to occur? How did your decision making and organizational processes perform in the crisis? Will you be better prepared for the next attack?

Exercise 12: Select one of your adversaries (an organization, not an individual). What assets do they need to protect? In what ways are these assets vulnerable? How does this understanding affect your strategy?

already crammed with details of surveillance and informing. As a kind of epilogue...

These are the documents which tell us how much an execution cost the czarist judicial system. They are the receipts signed by all those who collaborated, directly or indirectly, with the hangman.

All in all, not very expensive. The sums to the priest and the doctor are especially modest. The priesthood of the one and the profession of the other after all surely imply devotion to humanity.

At this point we should perhaps have a chapter headed: "Torture." All police forces resort in varying degrees to medieval "interrogation." In the United States they practice the terrible "third degree." In most European countries, torture has become generalized because of the resurgence of the class struggle following the war. The Romanian security services, the Polish Defense Ministry, the German, Italian, Yugoslavian, Spanish and Bulgarian police—and there must be others we have missed out—frequently resort to it. The Russian Okhrana preceded them in this, though with a certain degree of moderation. Although there were cases, even many cases, of corporal punishment (the knout) in the prisons, the treatment the Russian police meted out to prisoners before the 1905 revolution seems to have been generally more humane than is the case today when workers are arrested in any one of a dozen European countries. After 1905, the Okhrana had torture chambers in Warsaw, Riga, Odessa and apparently in most of the great urban centers.

Expenses for the execution of the brothers Modat and Djavat Mustafiu Oglu, sentenced to death by the court-martial of the Caucasus

Expenses	Cost in rubles
Transportation of the condemned men from the Metek fortress to the prison, paid to the carters	4
Other expenses	4
For having dug and filled in two graves (six grave diggers each signed a receipt for 2 rubles)	12
For setting up the gallows	4
For supervising the job	8
Traveling expenses for a priest (return)	2
To the doctor, for the death certificate	2
To the hangman	50
Hangman's traveling expenses	2

conclusion: why the Russian Revolution was still invincible

The police had to see everything, know, understand and have power over everything. The strength and perfection of their machinery appears all the more terrible because of the unsuspected resources they dragged up from the depth of the human soul.

But nonetheless they were powerless to prevent what happened. For half a century they vainly defended the autocracy against the revolution, which grew stronger every year.

It would in fact be wrong to let oneself be taken in by the apparently perfect mechanism of czarist security. It is true that at the top there were some intelligent men, technicians of high professional standing; but the whole machine rested on the work of a mass of ignorant civil servants. In the best-prepared reports some quite amusing discrepancies appear. Money oiled the wheels of this enormous machine; and gain is a strong but inadequate stimulus. Nothing great is achieved without disinterestedness. And the autocracy had no disinterested supporters.

Should it still, after the overthrow of March 26, 1917, be necessary to demonstrate, with facts taken from the history of the Russian Revolution, that the efforts of the head of the Police Department were in vain, we could quote a whole number of arguments like that put forward by the ex-policeman M.E. Bakai. In 1906, after the suppression of the first revolution, when the Chief of Police, Trusevich, re-organized the Okhrana, the revolutionary organizations of Warsaw, and in particular the Polish Socialist Party,¹³ in the course of the year liquidated 20 military, seven constables and 56 policemen and wounded 92; in all, they put 179 officers out of action. They also destroyed 149 consignments of excise alcohol. In the preparation of these actions hundreds of men took part, most of them remaining unknown to the police. M.E. Bakai observes that, in periods of revolutionary upsurge, agents provocateurs often lay low; but they reappeared as reaction gained the upper hand, like carrion crows over the battlefields.

In 1917, the autocracy fell without the legions of informers, provocateurs, hangmen, policemen, civil guards,

cossacks, judges, generals and priests being able to deflect the unswerving course of history. The reports from the Okhrana, written by General Globachev, affirm that the revolution is close at hand and offer the czar vain warnings. Just as the most knowledgeable doctors called to a deathbed can only observe, minute by minute, the progress of the disease, the omniscient police of the Empire watched impotently as the world of czarism plunged into the abyss.

For the revolution was the outcome of economic, psychological and moral causes outside their reach. They were doomed to resist helplessly and then succumb. Because it is the eternal illusion of the ruling classes to think that they can remove the effects without getting to the causes, legislate against anarchy or against syndicalism (as in France and the United States), against socialism (as Bismarck did in Germany), or against communism, as they strive to do more or less everywhere today. The same old historical experience. The Roman Empire too persecuted the Christians in vain. Catholicism had people burned at the stake throughout Europe, without defeating the heresy which is the essence of life.

In fact, the Russian police were overtaken by history. Instinctively, or consciously, the overwhelming majority of the population gave their sympathy to the enemies of the *ancien régime*. Their frequent martyrdom brought them some recruits and the admiration of countless others. Among the people, Christians for long centuries, there was an irresistible attraction towards the apostolic life of the propagandists who, renouncing comfort and security, faced prison, Siberian exile and death itself to bring the new evangel to the oppressed.

They were the real "salt of the earth": they were the best, the only bearers of an immense hope, and for this they were persecuted.

On their side they had the only moral strength, the strength of ideas and feelings. The autocracy was no longer a living principle. No one believed it was necessary. It no longer had any ideologies. Even religion, in the voices of its most sincere thinkers, condemned a regime which now rested solely on the systematic use of violence. The greatest Christians of modern Russia, the Dukhobors and Tolstoyans, were anarchists. But a society which no longer rests on living ideals, and whose basic principles are dead, often survives for a time by sheer weight of inertia.

But in Russian society in the last years of the *ancien régime*, the new, subversive ideas had acquired irresistible force. Everyone in the working class, the petty bourgeoisie, the army and the navy, the liberal professions—everyone who acted and thought—was a revolutionary, that is, a "socialist" of some kind. There was no satisfied middle bourgeoisie as in the countries of Western Europe. The *ancien régime* was no longer really defended by anyone except the upper clergy, the court nobility, the financiers, and a few politicians, in other words, by a very small aristocracy. Revolutionary ideas therefore found fertile soil everywhere. Over a long period, the nobility and the bourgeoisie gave the flower of their youth to the revolution. When a revolutionary went into hiding, he found many spontaneous, disinterested, devoted helpers. When he was arrested it happened more and more frequently that the soldiers in charge of conveying him sympathized with him, and among the jailers he sometimes found "comrades." So much so that in most prisons it was easy to communicate

illegally with the outside world. This sympathy also made escape easier. Gershuni, condemned to death and transferred from one prison to another, found policemen who became "friends." Burtzev, in his fight against provocation, gained valuable collaboration from a high-ranking official of the Ministry of the Interior, a Mr. Lopukhin, who happened to be an honest man, and from a former policeman, Bakai. I knew a woman revolutionary who had once been a prison warder. Cases of "screws" who were converted by prisoners were not at all rare. As an index of the attitude of the most backward elements of the population—from a revolutionary point of view—these facts are symptomatic.

And these are only the apparent, superficial causes, superimposed on other, deeper ones. The power of ideas, the moral strength, organization and mentality of the revolutionaries were only the results of an economic situation that was developing toward revolution. The Russian autocracy incarnated the power of an aristocracy of great landowners and a financial oligarchy subjected to foreign influences, which were in turn hampered by the existence of institutions so unfavorable to the development of the bourgeoisie. Few in number, deprived of political influence, and discontented, the middle class of the towns gave their children—student youth and intellectuals—to the revolution, a liberal revolution of course, not seeing the workers and *muzhiks* [peasants] coming up the line. The great industrial, commercial and financial bourgeoisie was restless, wanting an "English-style" constitutional monarchy, in which power would naturally fall to them. Weighed down by taxes, a prey in peacetime, in the period of great prosperity in Europe to periodic famine, demoralized by the vodka monopoly, brut-

ally exploited by the priest, the policeman, the bureaucrat and the big landowner, the rural masses, after over half a century, enthusiastically greeted the call of the revolutionaries who had forsaken their class: "Peasants, seize the land!" And as these masses supplied the army with the overwhelming majority of its ranks, the cannon fodder for Lyaoyang and Mukden, and the scourge of all uprisings, the army, with the military organizations of the clandestine parties working within it—this army kept in obedience by the courts-martial and the "gagging regime"—was in a ferment of bitterness. A working class still young, multiplying as fast as capitalist industry developed, deprived of consciousness, organizations, a press (rights not recognized by the old regime in Russia), oblivious to the attraction of the parliamentary regime, living in hovels, on low wages, the target of arbitrary police action—in short, faced with the bare reality of the class struggle—this working class became more and more clearly conscious of its interests with every day that passed. Thirty nationalities conquered or annexed by the Empire, deprived of the elemental right of speaking their own languages, or of the possibility of maintaining their own culture, Russified under the whip, were only kept under the yoke by constant repressive measures. In Poland, in Finland, in the Ukraine and the Baltic countries, in the Caucasus, national revolutions were in gestation, preparing to join forces with the agrarian revolution, the workers' revolution, the bourgeois revolution. The Jewish question was coming up everywhere too.

Holding the reins of power was a degenerate dynasty surrounded by imbeciles. The hairdresser Philip treated the shaky health of the heir presumptive by hypnotism. From his private council rooms, Rasputin removed and set up

ministries. The generals robbed from the army, the high dignitaries plundered the state. Between this power and the nation stood a countless bureaucracy, well oiled with bribes.

In the midst of the masses were the revolutionary organizations, broad-based and disciplined, constantly active, possessing both vast experience and the prestige and support of a magnificent tradition.

Such were the profound forces working for the revolution. And it was against them, in the vain hope of stemming the avalanche, that the Okhrana stretched its spindly strands of barbed wire!

In this deplorable situation, the police worked skillfully. Fair enough. They would manage, for example, to "liquidate" the Riga Social Democratic organization. Seventy would be taken prisoner, beheading the movement in the area. Imagine for one moment what total "liquidation" means. No one escaped. And then?

For a start, the imprisonment of the 70 did not go unnoticed. Each of the members was in contact with at least 10 people. Seven hundred people, at least, were suddenly faced with the brutal fact of the seizure of honest, brave people, whose only crime was to strive for the common good. The trial, the sentences, the private dramas involved, brought about an explosion of interest and support for the revolutionaries. If even one of them was able to make his impassioned voice heard from the dock, it could be said with certainty that the organization, at the sound of this voice, would rise again from the ashes. It was only a question of time.

And then what was to be done with the 70 members in prison? They could only be locked up for a long time or

deported to the deserted regions of Siberia. Very good. But in prison—or in Siberia—they find comrades, teachers and pupils. Their enforced leisure obliges them to study, to shape their theoretical ideas. Suffering together, they grow harder, become tempered, impassioned. Sooner or later, escaping, amnestied—through general strikes—or paroled, they will return to the life of society as “veteran” revolutionaries, “illegal” this time, and much stronger than ever. Not all of them of course. Some of them will die on the way; a painful selection process, useful in its own way. And the memories of friends who disappeared will make those who survive intransigent.

In the end, a liquidation is never completely final. The precautions of the revolutionaries will preserve some. The interests of provocation in themselves require some of the prisoners to be liberated. And chance operates in the same way. The ones who “escaped,” although they find themselves in difficult situations, are soon able to take advantage of favorable circumstances...

Repression can only really live off fear. But is fear enough to remove need, thirst for justice, intelligence, reason, idealism—all those revolutionary forces that express the formidable, profound impulse of the economic factors of a revolution? Relying on intimidation, the reactionaries forget that they will cause more indignation, more hatred, more thirst for martyrdom, than real fear. They only intimidate the weak; they exasperate the best forces and temper the resolution of the strongest.

And the provocateurs?

At first sight, they can cause the revolutionary movement

terrible losses. But is this really so?

Due to their help, the police can, of course, multiply their arrests and the “liquidation” of groups. In given circumstances, they can counter the most carefully laid political plans. They can do away with valiant militants. Provocateurs have often been the direct suppliers of the hangman. This is, of course, all terrible, but it is also the case that provocation can only wipe out individuals or groups and that it is almost impotent against the revolutionary movement as a whole.

We have seen how an agent provocateur became responsible (in 1912) for bringing Bolshevik propaganda into Russia; how another (Malinovsky) gave speeches written by Lenin in the Duma; how a third organized the execution of Plehve. In the first case, our agent could hand over a considerable quantity of literature to the police; but nonetheless he could not, for fear of blowing his cover at once, hand over all the literature, or even more than a limited quantity. Willy-nilly, he did contribute to the circulation. Whether a propaganda leaflet is handed out by a secret agent or a devoted revolutionary, the results are still the same: the essential thing is that it should be read. Whether Plehve’s execution was prepared by Azev or Savinkov doesn’t matter to us. It does not even matter whether it was the result of a struggle between different factions of the police; the important thing is that Plehve disappeared. The interests of the revolution in this case are much more important than those of the wretched little Machiavellis of the Okhrana. When the secret agent Malinovsky acted as Lenin’s voice in the Duma, the Minister of the Interior was wrong to rejoice over the success of his hired agent. Lenin’s words were far more important to the

country than the mere voice of a wretch like him. We can, thus, give two definitions of an agent which are complementary, but of which the second is much more significant:

1. The agent provocateur is a fake revolutionary
2. The agent provocateur is a policeman who serves the revolution in spite of himself — because he must always appear to be serving it

But in this question there are no appearances. Propaganda, fighting, terrorism, is all reality. There is no way you can be a member halfway, or superficially.

Wretches who in a moment of cowardice threw themselves into this swamp paid for it. Recently, in his *Unlittinly Thoughts*, Maxim Gorki published a curious letter from an agent provocateur. What the man wrote was something like this: "I was conscious of my baseness, but I also knew that it could not for a single second hold back the triumph of the revolution."

What is certain is that provocation poisons the struggle. It incites people to terrorism, even to terrorism of a type revolutionaries prefer to abstain from. What is really to be done with a traitor? The idea of pardoning him occurs to no one. In the duel between the police and the revolutionaries, provocation adds an element of intrigue, suffering, hatred and contempt. Is it more dangerous to the revolution than to the police? I think not. From another standpoint, the provocateurs and the police have a direct interest in ensuring that the revolutionary movement, which is their *raison d'être*, should always be a threat. In case of need, rather than give up a second source of earnings, they hatch plots themselves, as we have seen. In such cases, the interests of the police are completely in contradiction with those of the regime which

it is their job to defend. The maneuvers of such provocateurs can in a certain sense also be dangerous to the state itself. Azév once organized an attempt on the czar's life, which was frustrated only by totally fortuitous and unforeseen circumstances (one of the revolutionaries renouncing the plan). At that instant, Azév's personal interest — which was undoubtedly much dearer to him than the security of the Empire — demanded a bold action; within the Socialist Revolutionary Party he was under a cloud of suspicion which placed his life in danger. On the other hand, it has been raised that the attacks he successfully carried out might have served the designs of some Fouché. It is possible. But such intrigues among those in power only reveal the gangrene of a regime and contribute in no small measure to its fall.

Provocation is much more dangerous in terms of the distrust it sows among revolutionaries. As soon as a few traitors are unmasked, trust disappears from within the organizations. It is a terrible thing, because confidence in the party is the cement of all revolutionary forces. Accusations are murmured about, then said out loud, and usually they cannot be checked out. This causes enormous damage, worse in some ways than that caused by provocation itself. Recall these harrowing cases: Barbès made an accusation against the heroic Blanqui — and Blanqui, in spite of his 40 years of solitary confinement, in spite of his exemplary life and his indomitability, could never get rid of the infamous slander. Bakunin was also accused. And what about the victims who were less well known, but not less harmed by slander? Griet-Lorion, the anarchist, was accused of provocation by the "socialist" deputy Delory; to free himself of this intolerable suspicion, he shot the agents and was taken off to die in

prison. Another who met the same fate was also a valiant anarchist, from Belgium: Hartenstein-Sokolov (of the Ghent trial of 1909), who was vilely smeared by the whole socialist press and died in prison as a result. There is a tradition of it: the enemies of action, the cowards, the well entrenched ones, the opportunists, are happy to assemble their arsenal—in the sewers! Suspicion and slander are their weapons for discrediting revolutionaries. And we have not seen the end of it yet.

This evil of suspicion and mistrust among us can only be reduced and isolated by a great effort of will. It is necessary, as the condition of any victorious struggle against real provocation—and slanderous accusation of members is playing the game of provocation—that no one should be accused lightly, and it should also be impossible for an accusation against a revolutionary to be accepted without being investigated. Every time anyone is touched by suspicion, a jury formed of comrades should determine whether it is a well-founded accusation or a slander. These are simple rules which should be observed with inflexible rigor if one wishes to preserve the moral health of revolutionary organizations.

And what is more, however dangerous it is for the individuals concerned, the strength of the agent provocateur should not be overestimated: to a large extent, it is also up to every member to defend himself properly.

The Russian revolutionaries, in their long struggle against the police of the *ancien régime*, had acquired a very sure, practical knowledge of the procedures and methods of the police. If the police were very strong, they were stronger still. Whatever the perfection of the tables drawn up by the

Okhrana specialists on the activity of a given organization, it is certain that it contains gaps. As we said, "liquidation" of a group was rarely complete, because through their precautions, someone would escape. In the highly laborious diagram of Boris Savinkov's connections, some names are missing; and perhaps the most important ones. The Russian revolutionaries in fact considered that clandestine (illegal) action was subject to unbending rules. At every turn they asked themselves: "Is this in line with the rules of conspiracy?"¹⁴ The "code of conspiracy" had outstanding theoreticians and practitioners among the great enemies of the autocracy and of capital in Russia. It would be extremely useful to study this in depth. It must contain the simplest rules, precisely those which, because they are so simple, are often forgotten.

Thanks to this science of conspiracy, the revolutionaries were able to live illegally in the main cities of Russia for months or years at a time. They were able to turn themselves, as the case required, into peddlers, coachmen, "rich foreigners," servants, etc. In each case they had to live out their roles. To blow up the Winter Palace, the worker Stepan Khalturin¹⁵ spent weeks living the life of the workers employed at the palace. In order to keep watch on Plehve in Petrograd, Kaliaev became a coachman. Lenin and Zinoviev, hunted by Kerensky's police, were able to find a hiding place in Petrograd and only went out in disguise—Lenin as a factory worker.

Illegal action, over a period, creates habits and an outlook which can be considered the best guarantee against police methods. What talented police, what clever impostors can be compared with revolutionaries who are sure of themselves, circumspect, thoughtful and valiant, who obey a common

watchword?

Whatever the perfection of the methods used by the police to keep track of revolutionaries, won't there always be an irreducible unknown in their movements and actions? Won't there always be, in the most carefully worked out equations of the enemy, an enormous, fearful "x"? What traitor, what skilled informer or spy can decipher revolutionary intelligence? Who can measure the strength of revolutionary will?

When you have on your side the laws of history, the interests of the future, the economic and moral needs which lead to revolution; when you know with certainty what you want, what arms you have and what the enemy has; when you have decided on illegal action; when you have confidence in yourself and you work only with those in whom you have confidence; when you know that revolutionary work demands sacrifices and that every lovingly sown seed will bear fruit a hundred times over, then you are invincible.

The proof of this is that the thousands of Okhrana files, the millions of notes from the information services, the magnificent diagrams by its technicians, the works of its scientists, the whole amazing arsenal, is now in the hands of the Russian communists. The police, on the day of revolt, fled the cries of the crowd; those who were caught by the coattails took a dive—for good—into the canals of Petrograd. In the main, the officers of the Okhrana were shot.¹⁶ All the provocateurs who could be identified met the same fate. And one day, partly to show to the foreign comrades, we set up in a kind of museum a number of particularly interesting items taken from the secret archives of the police of the Empire. Our exhibition took place in one of the finest halls of the Winter

Palace; the visitors could leap through, by a window between two malachite columns, the jail book of the Peter and Paul Prison, the somber Bastille of the czars, over whose ancient battlements, on the other side of the river Neva, they could see the red flag flying.

Those who saw it know that even before it has conquered, the revolution is invincible.